2015

Virtue Ethics: Examining Influences on the Ethical Commitment of Information System Workers in Trusted Positions

John Max Gray
Nova Southeastern University, jg1553@nova.edu

NSUWorks Citation

John Max Gray. 2015. *Virtue Ethics: Examining Influences on the Ethical Commitment of Information System Workers in Trusted Positions.* Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (364) http://nsuworks.nova.edu/gscis_etd/364.

Virtue Ethics: Examining Influences on the Ethical Commitment of Information System Workers in Trusted Positions

by

John Gray

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2015

We hereby certify that this dissertation, submitted by John Gray, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Gurvirender P. Tejay, Ph.D.
Chairperson of Dissertation Committee — Date

Gurvirender P. Tejay, Ph.D.
Chairperson of Dissertation Committee

Date

Maxine S. Cohen, Ph.D.
Dissertation Committee Member

Date

Steven R.Terrell, Ph.D.
Dissertation Committee Member

Date

Approved:

Amon B. Seagull, Ph.D.
Interim Dean, College of Engineering and Computing

Date

College of Engineering and Computing
Nova Southeastern University

2015

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Virtue Ethics: Examining Influences on the Ethical Commitment of Information System Workers in Trusted Positions

by
John Gray
October 2015

Despite an abundance of research on the problem of insider threats, only limited success has been achieved in preventing trusted insiders from committing security violations. Virtue ethics may be an approach that can be utilized to address this issue. Human factors such as moral considerations impact Information System (IS) design, use, and security; consequently they affect the security posture and culture of an organization. Virtue ethics based concepts have the potential to influence and align the moral values and behavior of information systems workers with those of an organization in order to provide increased protection of IS assets. An individual's character strengths have been linked to positive personal development, but there has been very little research into how the positive characteristics of virtue ethics, exhibited through the character development of information systems workers, can contribute to improving system security. This research aimed to address this gap by examining factors that affect and shape the ethical perspectives of individuals entrusted with privileged access to information.

This study builds upon prior research and theoretical frameworks on institutionalizing ethics into organizations and Information Ethics to propose a new theoretical model which demonstrates the influences on Information Systems Security (ISS) trusted worker ethical behavior within an organization. Components of the research model include ISS virtue ethics based constructs, organizational based internal influences, societal based external influences, and trusted worker ethical behavior. This study used data collected from 395 professionals in an ISS organization to empirically assess the model. Partial Least Squares Structural Equation Modeling was employed to analyze the indicators, constructs, and path relationships. Various statistical tests determined validity and reliability, with mixed but adequate results. All of the relationships between constructs were positive, although some were stronger and more significant.

The expectation of the researcher in this study was to better understand the character of individuals who pose an insider threat by validating the proposed model, thereby providing a conceptual analysis of the character traits which influence the ethical behavior of trusted workers and ultimately information system security.

Acknowledgements

First and foremost I would like to thank Dr. Gurvirender Tejay for guiding my interest in ethics into a specific area that has applicability to information system security and refocusing me when my ideas took me out into left field. His mentorship, advice, uncompromising standards, and commitment to quality and relevance contributed immeasurability to this work. Thanks to my committee members, Dr. Cohen and Dr. Terrell. The quality of this dissertation is a direct reflection of their timely and valuable feedback.

To all of the DISS students termed as "Tejay's disciples" who participated in countless meetings at the Flight Deck and local area restaurants discussing information system security issues and research ideas late into many an evening. Dr. Tejay's facilitation and guidance of those discussions eventually provided that "a-ha" moment which crystalized not only my own research idea, but that of many other of his students, ultimately leading to their dissertation topic. In some ways these after-hours brain storming sessions contributed more to completing this work than any of the in-class activities.

Thanks to the Masonic fraternity and specifically my brothers in William H. Upton Naval and Military Lodge #206 for teaching me, albeit unknowingly, the concepts and power of virtue ethics. The lessons taught me through the various allegories of the fraternity improved me immeasurably. Halfway into this research I realized that the gentle lessons of the craft had a significant impact on this work and, as it should be - my life.

I want to express my gratitude to my colleagues in the NUWC Keyport IA and Cyber-Security Branch who patiently endured my discussions of ethics and provided invaluable input and critique of my ideas. I would like to specifically thank the management team of the Advanced Skills Management (ASM) software project, whose work practices inspired me to consider how ethics affected information system security.

Thanks to all the individuals who participated in my survey. I have a newfound respect for the effort involved in obtaining the required number of participants.

To the makers of craft beer and cigars, my indulgence of which provided me the quiet time to contemplate many ideas which manifested themselves in this research.

Thanks to my wife Bethany for patiently accepting that a portion of her life would be sacrificed in support of a goal of mine. I am forever grateful for your support. I promise – no more school! Also to my mother, Judith Sullivan of Spencer, IN, who inspired me to excel. Rest in peace Mom.

Finally, thanks to God for giving me the inner strength to complete what at times seemed an insurmountable task. "Remember now thy creator in the days of thy youth…"

"To educate a man in mind and not in morals is to educate a menace to society."
- Theodore Roosevelt

"Waste no more time arguing about what a good man should be. Be one."
- Marcus Aurelius

Table of Contents

Chapters

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

1.1 Background

Businesses and organizations are increasingly dependent upon information systems to maintain and control intellectual property, business sensitive, and classified information. While these systems are threatened by a variety of attackers, the greatest threat is of that posed by trusted insiders, those individuals who have legitimate access to the Information System (IS) (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005; Warkentin & Willison, 2009). System administrators, networking technicians, programmers, users with access to sensitive or classified information, information assurance, and information system security personnel all hold positions of trust, have legitimate access to systems, and are tasked with protecting organizational data and Information Technology (IT) assets. Most have some degree of physical access to, or administrative or elevated privileges; consequently these personnel, known as insider threats, pose the most significant threat to the IS and its data (Leach, 2003; Okolica, Peterson, & Mills, 2008; Warkentin, & Willison, 2009). Trusted workers who attack an IS understand the system security protections and typically do not arouse the suspicions of co-workers (Magklaras, Furnell, & Brooke, 2006).

Almost all modern organizations rely on information systems to conduct operations, and this pervasive use means that most organizations are vulnerable to trusted insider threats. Malicious actions by trusted insiders can result in serious damage to an IS, loss or compromise of data, denial of services, or damage to the organization’s reputation. One example of the serious harm to businesses presented by trusted insiders involved the US based software firm Ellery Systems, which had their entire proprietary software source code stolen by an employee who subsequently transferred it to a competing business in China. The resulting competition by the Chinese firm forced Ellery Systems out of business (Magnan, 2000). Another example of the damage an insider threat can cause was that of Yung-Hsun Lin, a disgruntled system administrator for a medical health care company located in the United States (US) who for vindictive reasons embedded malicious software code onto his employer's servers. Upon being activated the malicious code caused millions of dollars of damage and loss of data which subsequently impacted pharmacists' abilities to check for patient prescription drug interactions, thereby placing patient lives at risk (Marino, 2008).

One of the most infamous examples of the damage a trusted IS insider can cause is that of US Army intelligence analyst Private Bradley Manning. His IS access privileges enabled him to copy tens of thousands of sensitive and classified documents onto removable media which he subsequently supplied to WikiLeaks, a public website dedicated to whistle-blowing activities that publishes sensitive and classified information received from anonymous sources. According to the US Secretary of Defense the release of the documents by Manning caused severe damage by increasing the danger to the lives of US military personnel and damaging the country's international reputation. Additionally, the exposure of the details regarding foreign nationals collaborating with US forces in Afghanistan and Iraq placed the lives of those collaborators and their families in extreme danger (Amorosi, 2011). Even after incorporation of numerous technical controls and formal policies put into place by the US government after the

Manning incident, in 2013 Edward Snowden - an IT security analyst and systems administrator for the National Security Agency (NSA) was able to obtain and divulge classified documents and information to news agencies regarding various covert NSA surveillance programs. The information regarding those programs resulted in significant damage to the reputation and relationships of the US government both domestically and internationally (Landau, 2013).

Insider threats are not limited to employees filling technical or lower management positions. Numerous instances of lapses in ethical judgment by persons in significant leadership positions have cost their companies hundreds of millions of dollars in damages. Senior executives, by virtue of their powerful management positions have the ability to affect security policy implementation and oversight (Kraemer, Carayon, & Clem, 2009). Any decisions they make regarding configuration, operation, or management of the IS can affect security. They have the capability of inflicting significant damage to the organization such as in the Tyco International corporate scandal in which deceptive accounting practices by the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) nearly destroyed the company (Sogbesan, Ibidapo, Zavarsky, Ruhl, & Lindskog, 2012; Taylor, 2008); or even to the point of causing the company failure as demonstrated in the cases of Enron Corporation and WorldCom Incorporated (Lease, 2006). High profile cases involving senior executives of information systems include Robert Hanssen of the Federal Bureau of Investigation (FBI), a trusted worker who circumvented information system security in order to illegally obtain classified information which he subsequently sold to adversaries of the US, resulting in the compromise of numerous national security operatives and in the execution of several undercover agents located in the Soviet Union. His technical expertise in information technology and privileged access were key factors in being able to operate undetected for over 20 years. Hanssen was termed by the US Department of Justice as being the most damaging FBI insider in history (Magklaras et al., 2006).

Worldwide losses due to cyber-attacks are estimated at hundreds of billions of dollars (D’Arcy & Herath, 2011; Dorantes, Hewitt, & Goles, 2006). According to Greitzer et al. (2008) over 50% of IS security managers report significant financial losses due to insider intrusions and inappropriate computer use, and that insiders were responsible for over 85% of the breaches into DOD information systems. Herath and Rao (2009) also report huge losses due specifically to unethical activities by employees. The financial impact is most likely larger than publicized as it is estimated that only one in every 100 losses are reported. While external threats receive most of the attention in the press and are what most organizational security budgets and controls are directed at addressing, no external attack has ever resulted in the business failure of a major company. However, IS abuses and compromises by trusted insiders, usually by personnel in senior management or executive positions, have caused the collapse of numerous companies including Barings Bank, Enron, and WorldCom (Colwill, 2009). Hart (2001) considers this evidence that organizational leadership positions are not being filled by people who possess good character.

Information policy has been defined as the rules, laws, and guidelines put in place to facilitate the collection, organization, dissemination and use of information (Yusof, Basri, & Zin, 2010). Policies should provide overall guidance, not inhibit business or organizational operations, and should delineate what type of information needs to be controlled as well as the level of control desired. Despite their pervasive use, failure of information policies to control and protect information is seen as a key threat to the governing organizations from various standpoints including those of national security and stability, protection of economic interests, and protection of cultural values (Siponen, Pahnila, & Mahmood, 2010). In particular, the use of IS policies, technical solutions, and access controls have proven to be ineffective against trusted insiders who are motivated to compromise the system or its information (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Colwill, 2009). Performing malicious acts can be attributed to the ethical commitment of trusted IS workers, and formal policies and technical solutions will not solve these human issues (Kraemer et al., 2009). Investigation into what affects insider motivations and how their motivations can be influenced is called for in order to develop new methods of addressing the associated vulnerabilities, threats, and risks.

1.2 Research Problem and Argument

The research problem is that there is an urgent need for organizational management to better understand the problem of insider threats to information systems in order to prevent trusted worker unethical behavior (Colwill, 2009; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005; von Solms, 2006). Management must explore ways to understand, influence, and align the moral values and behavioral intentions of information systems workers with those of the organization so as to provide increased protection of information systems data assets.

The argument of this research is that a new approach such as virtue ethics must be considered and key elements of virtue ethics identified which influence the decision making processes of information systems security trusted workers. This was pursued by confirming through statistical validity four proposed virtue ethics based constructs as they relate to ISS. A theoretical ethical behavior model was evaluated, thereby providing a conceptual analysis of the character traits which may influence the ethical behavior of trusted workers and ultimately information system security.

Virtue ethics emphasizes the importance of traits of character that define a morally good individual and which affects their ethical decision making. Pollack and Hartzel (2006) note that how individuals use information they are entrusted with is solely determined by their beliefs, ethics, and values. Previous research concludes that moral considerations and decisions impact IS design, use, and security; consequently they affect the security posture and culture of the organization (Hu, Hart, & Cooke, 2007; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Pahnila, Siponen, & Mahmood, 2007; von Solms, 2000). When presented with ethical situations and decisions that impact IS security, motivated trusted insiders desiring to violate security can easily circumvent existing security controls. An individual’s decisions are shaped by ethics and norms, and the factors that influence decisions can be identified and therefore affected by other influencers such as leadership, training, and continual practice (Dyck & Wong, 2010; Grodzinsky, 2001; Hart, 2001; Kane & Patapan, 2006; Weber, 1981, 1993).

It can be countered that practitioners are best equipped to address IS security violations with technical controls, analytical tools, and auditing, and that these controls provide the security necessary to protect systems against internal as well as external threats (Baskerville, 1991; Saint-Germain, 2005). However, technology alone cannot detect or prevent insider threats. Past research has shown that that formal, technical, and action based normative controls designed to protect sensitive information and data assets fail to prevent trusted insiders from committing IS security violations (Colwill, 2009; Greitzer & Hohimer, 2011). Virtue ethics based concepts has the potential to influence and align the moral values and behavior of information systems workers with those of an organization in order to provide increased protection of IS data assets.

1.3 Importance of Research Problem

An individual’s attitudes and behaviors can affect information systems security (ISS). This could lead to compromise, loss, illegal or unauthorized access to, or the wrongful dissemination of sensitive data such as privacy or personally identifiable information, intellectual property, or classified material. Many organizations have instituted codes of conduct as a deterrent to undesirable behavior, but ethical issues continue to be a problem. Inability to execute corporate strategies, loss of stock value, loss of profits, or damage to the organization’s public reputation are all negative consequences that may result from ISS failures (Ekelhart, Fenz, & Neubauer, 2009). The conclusion is that an understanding of the ethical foundations of socio-organizational ISS can lead to the development of ethics based normative controls.

It has been shown through past ethical failures that an individual’s ethical commitment will likely override any organizational guidance provided through security training, directives, and policies. Information system workers employed in trusted positions who inadvertently neglect, exhibit a deliberate disregard or avoidance, commit passive or active resistance, make uninformed decisions, or display a disinterested or negative attitude towards ISS can negate even the best security policies, controls, and regulations (D’Arcy & Hovav, 2009; Dorantes, Hewitt, & Goles, 2006; Gerber & von Solms, 2008; Pahnila et al., 2007; Siponen, 2006; Workman & Gathegi, 2007). Additionally, their self-interests can have a bearing on system security matters which require ethical decisions. These factors can lead to negative actions by those motivated insiders including subversive acts that willfully circumvent or disregard security requirements or by directing and pressuring subordinate employees not to incorporate them. The result can be the avoidance, weakening, or circumvention of the implementation and effectiveness of security controls thereby placing the system or data at risk (Colwill, 2009; Dhillon & Torkzadeh, 2006; Hu et al., 2007; Myyry et al., 2009).

Normative ethics examines the rightness or wrongness of the ethical actions of individuals as they relate to the moral rules of society. The three primary approaches to normative ethics are consequentialism, which focuses on the goodness or consequences of actions; deontological, which focuses on duties and rules; and virtue ethics, which focuses on character traits (Chun, 2005; Dahlsgaard, Peterson, & Seligman, 2005; Dyck & Wong, 2010; Howe, 1990; Oderberg, 1999; Shanahan & Hyman, 2003). Virtue ethics based normative controls are used to induce increased commitment from individuals by appealing to their beliefs, emotions, thoughts, and values instead of actions and consequences which are influenced by a system of rewards and punishment. They are considered a prescriptive approach that can be used by organizations to institute cultural change with the goal of providing benefit to the organization by shaping the ethical makeup and subsequently the actions of employees (Moore, 2005a, 2005b; Trevino & Weaver, 1994). The information technology (IT) field has recognized the importance of ethical reasoning and its effects on the actions of groups and individuals. The ethical values of these individuals and groups and their ethical viewpoints and decisions are part of what comprises the ethical climate of an organization (Banerjee, Cronan, & Jones, 1998; Dhillon & Torkzadeh, 2006). This climate affects decisions about the protection of the organization's information systems and data. The use of virtue ethics provides a method for the development of individual character and ethics which will lead into professional ethical behavior. Normative controls based on virtue ethics present a unique approach to the challenge of protecting information systems and their assets (Adam & Bull, 2008; Dyck & Wong, 2010; Grodzinsky, 2001; Harris, 2008; Siponen & Iivari, 2006, Stamatellos, 2011a, 2011b).

1.4 Definition of Key Terms

Definitions of the key terms that form the core of this research study are necessary to provide familiarity and to avoid misunderstandings by the reading audience.

An *information system* is commonly thought of as a computer based system used to handle data. Liebenau and Backhouse (1990) extend this further, describing it as an aggregate of information handling activities at a technical, formal, and informal level in an organization; however this leaves room for vague or fuzzy interpretations. According to the National Institute of Standards and Technology (NIST, 2006) an information system is a collection of information resources including information technology equipment, funding, support services, and people organized to collect, process, maintain, and disseminate information; which implies that the system is comprised of tangible resources that may or may not involve computing machinery. A more unambiguous definition is that an information system goes beyond just the technical components, but consists of the entire set of activities, data, and persons that process, either through automation or manually, the information in an organization (Cartelli, Daltri, Errani, Palma, & Zanfini, 2009). The activities which involve the organization's personnel include making policy decisions that affect how information is handled, and may or may not directly involve the computer based system which stores and processes organizational data. This definition of an *information system* more accurately represents all aspects of how information within an organizational entity is handled and is the one which was used in this study.

Information system security has been described by Anderson (2003) as "a well-informed sense of assurance that information risks and controls are in balance" (p. 310). What is not addressed in this definition is that the balance of risks and security controls is subjective. Different observers or evaluators would see the likelihood and impact of risks and mitigation effects of controls differently, each with varying degrees of accuracy. Some risks may be known, but not the impact or severity, while some systems risks may have not yet emerged or are unknown, thereby resulting in a false sense of security. Achieving a balance is dependent upon all information being known and how accurately one assesses the risks. The weakness in Anderson's (2003) definition is that the informed sense of assurance that all risks and their impact are known is often incorrect (Bernard, 2007; Dhillon & Torkzadeh, 2006; Sun, Srivastava, & Mock, 2006). It is contended by Theoharidou et al. (2005) that information system security is protection of all elements of an information system including hardware, software, information, personnel, and processes. The inclusion of people as a component is important because the human element is often the cause of security breaches and failures. What is left unclear in this definition is what is meant by protecting the “people” element and if it addresses personal behavior. Dhillon and Torkzadeh (2006) recognize this and conclude that information system security consists of protecting an organization’s information resources through the use of technical and management controls, procedures, and by managing people’s behavior. This description is inclusive of the fact that all risks to a system may not be known, and that controlling the activities of individuals is key to security success. This is consistent with studies of past security failures, therefore Dhillon and Torkzadeh’s (2006) definition of *information system security* was adopted in this research.

The term *insider threat* has negative connotations, implying that an individual is working from within an organization to bring intentional harm. Maybury et al. (2005) agree with this, describing an insider threat as being an individual who is motivated to perform actions which adversely impact an organization by performing acts which compromise the confidentiality, integrity, or availability of its information. This implies that the insider performs the actions because they desire to cause outright harm to the organization; however, this fails to take into account that many insiders operate with other motivations, such as personal profit or misaligned personal allegiances. In these circumstances any overt harm to the organization is secondary and likely unintended. Threats from individuals who misuse the privileges they have been granted to an information system which consequently violate organizational ISS policies are termed insider threats by Theoharidou et al. (2005). In this interpretation it is left to question whether “misuse” by the individual is intentional or not. In the examination of insider threats by Colwill (2009) they are identified as employees who have either privileged access or legitimate authority to information, and who either accidently or intentionally through malicious acts compromise the confidentiality, integrity, or availability of that information by abuse, illegal actions, sabotage, or unauthorized release. This definition addresses all information resources, not only those maintained by computing machinery, but also those held in confidence by the individual. It also takes into consideration that while not all compromises may be intentional or committed with the intent of causing harm to the organization they still represent a threat to IS security. Considering the goal of ensuring ISS, this definition is accepted in this research as the best description of an *insider threat*.

A *trusted insider*, also referred to as a trusted worker, has been described as a person who is employed by an organization and has privileges to access its sensitive data. A somewhat restricting definition is used by Magklaras et al. (2006) who state that legitimate access to one or more components of an information system has been granted to the insider through interaction with an authentication mechanism—the use of which seems to limit considerations to the technological components of the IS. As has been established by previously cited research an information system is comprised of more than just the computing hardware and software, it also includes processes and people. Therefore the description of trusted insider by Magklaras et al. fails to address other information elements that the insider interacts with beyond that which resides on the computing machinery. A more encompassing description is that a trusted insider has knowledge of the IS and understands its network topology according to Althebyan and Panda (2007). Hunker and Probst (2011) describe a trusted insider as a person who has been legitimately empowered with the right to access, represent, or make decisions regarding the assets of an organization. With the understanding that an IS consists of resources organized to handle all aspects of an organization’s information, the Hunker and Probst definition of *trusted insider* is the most appropriate and is utilized in this study.

Virtues, the core concept of this paper, are demonstrated through the voluntary actions of an individual according to Aristotle (2005). It is maintained by Artz (1994) that virtues consist of personal qualities and character traits which contribute to the excellence of an individual. Hart (2001) and Whetstone (2001) assert that virtuous actions consist of three characteristics; that they are intentional acts by a person who is aware of important facts about a circumstance and who has the wisdom needed in which to take correct action, that the motive for performing the act is not driven by any perceived personal advantage or external rules or controls, and that the virtuous actions are not just a one-time event but are consistently displayed by the individual over time. However, the definition which best captures these ideas remains that described in MacIntrye’s (1984) landmark work on the subject of virtues, that *virtue* is an acquired quality or personal disposition which shapes the basic components of good character. By possession of and through repeated use of virtue an individual promotes self-knowledge, knowledge of goodness, and ultimately achieves internal and external good (MacIntyre, 1984). The conclusion is that virtues are acquired and that through continual use they will become part of a person’s character.

Ethics which are based on an individual’s character, development of personality, and human virtues are termed *virtue ethics* (MacIntyre, 1984). According to Whetstone (2001) virtue ethics place special emphasis on moral character development with the result that any subsequent decisions made by the person will be consistent with that character. Dyck and Wong (2010) expound on the concept by noting that virtue ethics are behaviors that when practiced shape a person's character, that past actions strongly influence that person's future actions, and that virtue ethics provide a useful method for examining the varying perspectives that drive people's actions. The definition which best exemplifies the idea of *virtue ethics* is that they are a group of personal traits and qualities that provide a foundation for a person to lead a virtuous life, and through repeated inculcation and practice these qualities are developed into habits which once acquired, ensure that when that person is presented with an ethical situation they will make the right choice. They mold character and are the cause of future actions (Duarte, 2008). This best describes virtue ethics as the theoretical approach referred to in this study.

1.5 Summary

This chapter presented an overview of the research goals, identified the research problem which was investigated, and provided a supporting argument. The relevance and significance of the proposed research is also presented in regards to the current threats to information systems by trusted insiders. The chapter concluded with a definition of key terms that are used throughout the proposed research.

Chapter 2

Literature Review

2.1 Introduction

The goal of this chapter is to present an overview of the relevant literature to provide background and context for the study, establish that the researcher was aware of and understood the existing body of knowledge in regards to the subject matter, corroborate the research problem, facilitate theory development, and identify where additional research may be needed.

There have been numerous studies on ethical behavior, behavior intentions, and the ethical use of computer systems. Ethics, organizational ethics, and the factors that drive the ethical behavior of employees have also been the focus of numerous research efforts (Drover, Franczak, & Beltramini, 2012; Sison, Hartman, & Fontrodona, 2012). Diverse literature on ethics and employees, particularly of information systems (IS) personnel and trusted insiders, was reviewed to provide context and background for this study. The literature review regarding ethical behavior, employee ethics – particularly that of IS personnel and trusted workers, ethics codes in organizations, information system security (ISS) socio-technical controls, and other factors that may contribute to the information system (IS) security culture in organizations also established a solid foundation on which to justify the study and validate the research approach. The chapter concludes with a summary of what is known and unknown regarding the topic.

2.2 Organizational Ethics

There has been a significant amount of research into the factors that influence the moral reasoning and ethical behavior of individuals in business organizations (Weber, 2010). Behavioral intention, which is based on the individual’s attitude regarding both the behavior and any relevant subjective norms, is one of the best ways for predicting an individual’s ethical behavior and is an indication of an individual's readiness to perform a given behavior (Ajzen, 1991; Weber & Gillespie, 1998). A subjective norm is predicted by the individual’s belief about what other people such as a manager, would advise regarding an action and by an individual’s motivation to comply. Behavioral intentions can predict a person’s behavior and along with ethical beliefs can be used to understand and predict group and individual behaviors in specific situations (Weber, 2010; Wood-Harper, Corder, Wood, & Watson, 1996).

Loch and Conger (1996) found that a person’s feeling of anonymity affects their computing behaviors and intentions but they call for more research into individual characteristics in order to fully define an individual’s roles in ethical decision making. They also postulated that an individual’s attitudes and behaviors are affected by ones intentions in ethical issues. Donner (2003) goes further, stating that many feel that every decision made is affected and influenced by a person’s ethics and concludes that an individual’s feelings rather than logic often determine the decisions they make.

While a person’s moral development stage determines how they think about ethical issues and the associated decisions, awareness of the concepts of right and wrong are not accurate predictors of the ethical choice a person will actually make (Trevino, 1986). There are also individual and situational factors that interact and influence how a person will respond to an ethical dilemma. Chun-Chang (2007) notes that an IS worker may have a positive attitude towards IS security, but the individuals actual behavior may be influenced by ethical standards that vary from situation to situation. Situational factors are those that are shaped by organizational culture and job context, and consist of a person's feelings of responsibility for consequences of actions, conformance to rules, obeying authority, and other pressures; and it is advocated by Trevino (1986) that the interaction of the individual and situational factors or variable can help explain how ethical choices are made. Trevino (1986) and Banerjee et al. (1998) define the individual factors of ego strength, an individual's strength of conviction and self-regulation abilities; locus of control, a person's perception of the amount of control that they can exert over events with some individuals believing they have significant control as a result of their efforts while other believe events are controlled by luck or fate; and field dependence, wherein a person attempts to reconcile ethical dilemmas by internally redefining them so that they seem ethical or convincing to themselves so that they will not be responsible for any negative results of an unethical action . Neither Trevino nor Banerjee et al. consider external influences on an individual's ethical choices.

An individual's attitude in regards to ethical behavior, perceived behavior control, and personal beliefs are the primary predictors of ethical behavior intention (Ajzen, 1991; Weber 2010). Perceived behavior control is how easy or difficult it is for the individual to perform the behavior. In his seminal research, Ajzen also suggests that a person's intentions, described as how hard they are trying or how much effort they are going to exert to perform a behavior, can be accurately foretold based those predictors. This implies that if an individual acts ethically in a certain situation, that they would always act ethically in that situation. This does not agree with the Banerjee et al. (1998) contention that different factors can cause different outcomes in the same situation. Van Niekerk and von Solms (2010) explored organizational values as they were documented in policy, the shared beliefs and assumptions of employees regarding successful security methods as related to their work, and the strength or weakness of particular values; however, a focus on ethics was missing. Ethics is one of the organizational work climates identified by Schneider and Reichers (1983) but their study, albeit dated, focuses mainly on the organization and implies that if there is an ethical climate in an organization then ethical behavior by employees will automatically follow.

Within an organizational culture the issues of ethics or values are important components because the values of the organization's members, particularly those in positions of influence, determine what values become institutionalized (Moore, 2005b). Despite the progress in identifying factors that influence moral reasoning and decision making in a business context, Weber (2010) concludes that a deeper understanding on how to institute ethics into an organization is called for. These issues are important because behavioral security, how people behave in regards to security issues, affects the overall IS security culture of an organization (Dhillon et al., 2007).

2.3 Virtue Ethics

Numerous researchers have identified the need for use of spiritual or religious based ethical frameworks and concepts to actualize positive changes within organizations (Dyck & Wong, 2010; Keller, Smith, & Smith, 2007). Ethical theories which are proactive in nature are termed constructionist, with virtue ethics being one of the best examples because it promotes the proper construction of a moral agent (Floridi &

Sanders, 2005). Virtue ethics focuses on development of desirable character traits rather than the results of actions as a basis for a person's morality (Artz, 1994; Moore, 2005a, 2005b). Virtues are lasting character traits which are manifested in a person's behavior, become associated with their personality (Harris, 2008), and according to Moore (2005a) enable a person to live up to their values. Furthermore, these virtues should be practiced in communities such as organizations (Dyck & Kleysen, 2001; Dyck & Wong, 2010). Harris (2008) goes further, stating that the deepest significance is found by a person integrating virtues into their entire life.

Also known as ethics of character, virtue ethics is one of the oldest forms of ethics, providing a philosophical perspective based on normative ethics (Bright, Winn, Kanov, 2014). It was developed in ancient Greece by the philosopher Plato, refined and championed by his student Aristotle, and extensively examined from a theological perspective by the 12th century Dominican priest and philosopher Saint Thomas Aquinas. Aristotle's concepts of virtues, which are based on Plato's cardinal virtues, focus on an individual's character, and when associated with experience they form values and enable the individual to act in a morally correct manner. According to Aristotle the central notion of ethics is virtue, with virtue being human excellence at a particular function that brings about good or desirable results. Aristotle also felt that the nature of virtue is that it is the peak of excellence between the extremes of deficiency and excess; that virtues are how people act, and are fashioned after repeated action that becomes habit. Aristotle (2005) stated that the goal of life is to reach a state of genuine happiness which requires achievement of virtue, and the doctrine of virtue is the self-understanding that an individual should strive to achieve through application of the virtues. Throughout history the dominant method of moral reasoning has been through the use of a virtue ethics based approach (Bright et al., 2014). Aquinas's comprehensive consideration of the virtues in the context of their relationship between faith and reason became an important part of Christian ethics (Harris, 2008). As a result of centuries of study this doctrine has been recognized as a key component of the European/Western consciousness (Pieper, 1966).

The use of virtue ethics to develop and shape the moral character and behavior of individuals has an established history in western society and has long been used by organizations. The 18th century saw the manifestation of the Age of Enlightenment, termed as unassisted reason, which constituted and fostered new guidelines and codes for human conduct (Mehigan & De Burgh, 2008). One of the key social institutions during this period was Freemasonry, a fraternal organization with a documented history dating to 1390 AD as evidenced by the Regis Manuscript. Freemasonry taught a system of individual morality and self-improvement based on the cardinal virtues or virtue ethics in order that its members could live better, happier, and wiser lives (Bragado, 2002). Masonic liberal thinking during this period instituted a program of ethical and moral social improvement which was used to promote equality and for individuals to pursue excellence by doing what was right, thereby achieving happiness, the goal of virtue ethics (Aquinas, 2005 & Aristotle, 2005). The various masonic rituals embodied the cardinal virtue doctrine using them to effectively instruct members in basic moral truths that could be used in everyday life (Cerza, 1968; Mehigan & De Burgh, 2008; Steinmetz, 1976). Through Freemasonry's cultivation of moral and ethical principles emphasis was placed on the individual, the choices the individual makes, personal growth, and moral development (Cochran, 1992). The cardinal virtues of temperance, fortitude, prudence, and justice were taught as part of the philosophy of Freemasonry so that the individual member could understand what the fraternity expected of him, to better know themselves, to understand their own strengths and weaknesses, and consequently to improve themselves morally (Spelman, 1996). The masonic fraternity prevails as the largest and oldest fraternal social institution in the world, using virtue ethics to instruct its membership.

Virtue ethics is more than a way of thinking about how to determine right or wrong behavior. They shape a person's values so that when an ethical choice is presented the deliberations over choosing are for the most part already over (Stamatellos, 2011a), therefore the act of making the ethical choice comes naturally because it is part of the person's character. Virtues help guide, motivate, and correct an individual's moral deliberations and actions (Whetstone, 2001, 2005) and practicing virtuous acts creates a virtuous character which once formed is no longer the outcome of the virtuous acts, but rather the cause of them. Ultimately a virtuous person will act autonomously with their actions based on internal determinations rather than on external factors or conditions. Virtuous acts should not be based on the action, but on the quality of the person performing it, their thoughts and contemplations, in short – the ethical virtue of the person (Stamatellos, 2011b). Through the use of virtue ethics an individual's character is the basis for their moral evaluations, personalizing and simplifying their ethical decisions; and is useful in addressing new and complex issues that arise in fields such as information systems (Artz, 1994; Stamatellos, 2011a).

Virtue ethics is based on the four cardinal virtues, cardo being the Latin word for "hinge", referred to as such because as conceived and explained by Aristotle and Aquinas all other human virtues hinge upon them. According to Hart (2001) the cardinal virtues cannot be derived from any other virtues, that all other virtues are derived from them, and that they represent the essential aspects of human nature. A person must have these four virtues before they can possess any others (Oderberg, 1999). The cardinal virtues as defined by Aquinas (2005) are:

Prudence: the application of wisdom or right reason regarding taking the appropriate action according to a given situation (Aquinas, 2005, pp. 2-3).

Fortitude: the strength to resist the difficulties which prevent proper action; an ability to confront and endure fear and uncertainty or intimidation (Aquinas, 2005, pp. 106).

Justice: regarding relationships between others, the perpetual and constant willingness to render to each individual what they rightly deserve; just or fair acts (Aquinas, 2005, pp. 30-33).

Temperance: practicing self-control, abstention, and moderation of actions, desires, and emotions (Aquinas, 2005, pp. 119- 120).

Nonetheless, numerous researchers have studied the works of Aristotle and Aquinas on the cardinal virtues and have interpreted and expounded upon the definitions of the virtues as well as assigning them additional measures or indicators. A review of notable past ethics research provided seminal contributions to the development of an amalgamated definition of each of the four virtues that were used in this study.

Prudence, also termed as practical wisdom, is characterized by Aristotle (2005) as a person making appropriate decisions to maximize good, and by Aquinas (2005) as when a person's undertakings are made through careful considerations; and by putting morally correct decisions into action. Dahlsgaard et al. (2005) determine that it involves the acquisition and use of knowledge, judgment, and perspective as well as providing good council to others. Dyck and Kleysen (2001) have a similar view, that prudence is the deliberate, good evaluations and actions made through the application of relevant knowledge, and to make decisions that increase the common good. Arjoon (2000) defines it as when a person exercises sound reason, while Dyck and Wong (2010) state that it is the consideration of the input from others when making decisions. According to Nash (1990) prudence is personal honesty and trustworthiness, and Oderberg (1999) defines it as good judgment when assessing right and wrong situations. Riggio, Zhu, Reina, and Maroosis (2010) conclude that prudence is a person's knowledge, insight, wisdom, and the application of honesty and experience when making right decisions. The viewpoint of Shanahan and Hyman (2003) is that prudence is a person doing the right thing, and being reliable and trustworthy when making decisions in order to minimize personal or organizational losses. Consideration of the prior research results summarizes the definition of prudence as when a person's considerations, judgments, and actions are based on knowledge, experience, and input from others; and that these considerations result in morally correct decisions.

Fortitude, also known as courage, is explained by Aristotle (2005) as the performance of acts by a person that could result in the loss of position or status. Aquinas (2005) states that fortitude is when a person chooses to do the right thing despite fear, has confidence when facing obstacles, or performs actions that are not governed by irrational fear or recklessness. Dahlsgaard et al. (2005) elaborate that fortitude is a person having emotional strength, perseverance, and exercising one's will when faced with opposition as well as being honest and authentic. Dyck and Kleysen (2001) note that resisting pressure, acting for the good of all, maintaining integrity at the expense of self, empowering others, and speaking up in matters of personal conviction and injustice are qualities of fortitude. Dyck and Wong (2010) add it also includes when a person implements unpopular or threatening changes. Achievement and reliability are also qualities of fortitude according to (Nash, 1990), while a person doing the right thing, having proper ambition, perseverance, patience, determination, being indifferent to petty things, and not being affected by trivial reasons from taking a particular course of action are measures identified by Oderberg (1999). Riggio et al. (2010) align with Aquinas in that fortitude is a person working with fear to do the right thing despite personal risk or sacrifice; as well as honesty, integrity, and being incorruptible despite pressure to do otherwise. Based on the finding of these researchers, a single definition of fortitude is derived as a person having the personal integrity and willpower to make ethically correct or unpopular decisions despite pressures to do otherwise, even if it results in little or no personal benefit, risks loss of personal position, or creates adversity.

The cardinal virtue of justice was defined by Aristotle (2005) as a person following laws and being fair with others, while Aquinas (2005) states that it governs right relationships and duties owed to other people. Shanahan and Hyman (2003) describe justice as treating others fairly and being sympathetic, generous, and caring for individuals and corporations. Riggio et al. (2010) see justice as when individual self-benefits are not achieved at the expense of others, and by a person being a good citizen. Respecting and obeying employers and superiors, keeping promises, respecting the private information and property of others, and remedying any harm caused through one’s own fault are measures identified by Oderberg (1999). Nash (1990) defines justice as having respect for others and displaying fairness and integrity; while Dyck and Wong (2010) state that it is being sensitive to the needs of the less fortunate. Dyck and Kleysen (2001) describe justice as fairness, giving credit where it is due, accepting advice from others, and demonstrating personal responsibility within an organization. Dahlsgaard et al. (2005) also identify fairness, as well as by a person being a good citizen, demonstrating leadership, teamwork, and civil strength that benefits a community. Considering the results of this research, an aggregate definition of the cardinal virtue of justice is that a person is sensitive to the rights of others and acts fairly and responsibly towards individuals, organizations, and communities.

The cardinal virtue of temperance is described by Aristotle (2005) as an individual having self-control and avoiding personal desires, and by Aquinas (2005) as humility, self-control, and moderation. Shanahan and Hyman (2003) conclude that it is when a person does not think too highly of themselves. Riggio et al. (2010) feel that a person’s control of emotions is key, while Oderberg (1999) concurs with other researchers that humility as well as moderation for self-glorification, modesty, punctuality, and a lack of idle curiosity defines temperance. Dyck and Kleysen (2001) identify a person’s emotional regulation, control of impulses, moderation of desires, maintaining integrity, not overreacting, preserving resources, and embracing larger perspectives as measures of temperance, while Dyck and Wong (2010) state that it is a person’s resistance of selfish influences. Dahlsgaard et al. (2005) identify forgiveness, humility, protection against excess, and self-control as traits. Nash (1990) differs, simplifying the definition as self-respect. With the prior research as a guide, a unified definition of temperance is that it is a person’s self-restraint in conduct, humility, and self-control of emotions and actions.

While some philosophers believe that an ethical course of action can be justified by only one theory, Whetstone (2001) advocates that there can be more than one reason for a person to commit a particular act, that virtue ethics can complement other ethics theories, and further recommends that organizational managers use virtue ethics to address the human behavior of their employees. Virtue ethics is not without criticism, it has been noted that various cultures differ on what traits are considered virtues (Whetstone, 2001), that it may not be as effective in multicultural groups, and rather than just thinking solely of the rightness of an action that they take, an individual practicing virtue ethics should also consider the consequences which result from that action (Stamatellos, 2011a). Huff and Frey (2005) note that many practitioners dispute that teaching morals is worth the time and effort.

Despite its criticisms, virtue is considered as one of the basic ethical concepts, therefore a focus on virtue ethics may be able to influence the individual and situational factors that impact a person’s ethical decision making process. The primary emphasis of virtue ethics is on the lifelong process of development of a person’s moral character (Whetstone, 2001, 2005), and by extension organizational virtue and culture (Dyck & Wong, 2010). Hart (2001) concurs, adding that the character improvement must be constant, intentional, and voluntary; and further argues that when all ethical systems are considered, virtue ethics is the one that is most compatible with human nature. Pieper

(1966) advocates that virtue ethics is considered as one of the most important discoveries in the history of human self-understanding. In short, the concept of virtue ethics is characterized by an individual having a moral commitment to what is good.

2.4 Ethics is Applicable to Information System Security

It is important to understand the culture of an organization and its employees in order to develop approaches that foster an effective information security climate and to understand an employee’s attitudes towards ethics (Vroom & von Solms, 2004). Changes can then be effected through employee acceptance rather than by enforcement methods that threaten negative consequences for non-compliance. The human factor has a significant influence on the effectiveness of information systems security (ISS) and because it cannot be adequately managed by formal or technical controls, an organizational culture of information security must be developed and promoted (Colwill, 2009; Dhillon & Backhouse, 2000; von Solms, 2000). Iivari (1991, 2007) concludes that ethical choices and decisions by individuals are a component of the system development process. Wood-Harper et al. (1996) as well as Cartelli et al. (2009) advocate that individuals are fundamental components of an IS, and that efforts to recognize various ethical views in a situation will result in a better understanding of the human element and its relationship to the IS.

Various ethics studies state that a failure to understand the human context has been the cause of many IS failures (Colwill, 2009; Jones, 1991). Ethics in general are seen as important by researchers and ethics problems affect the information security field because ethical decisions are routinely required (Dark, Harter, Morales, & Garcia, 2008;

Delany & Sockell, 1992). Research by D’Arcy and Hovav (2009) found substantial empirical evidence which indicates that moral considerations play a significant part in the misuse of an information system. Research by Eloff and Eloff (2003) notes that one way to approach information security management is by taking a human viewpoint to address human related issues such as ethics. Despite the emerging importance of ethics to ISs and their security, efforts to develop ethical climates in organizations are few (Mathieson, 2008). The implementation and use of information systems incorporates cultural and social aspects, therefore ethical issues apply to the discipline, but research into behavioral aspects as related to these systems is underexplored, and exploration of alternative ethical frameworks such as virtue ethics is overdue (Adam & Bull, 2008; Boss et al., 2009). Siponen (2004) echoes the need for new ethical theories in ISs and identifies Floridi’s Information Ethics theory as one that has been proposed. Floridi is a leading researcher in the field of information ethics which is defined as the “branch of ethics that focuses on the relationship between the creation, organization, dissemination, and use of information and the ethical standards and moral codes governing human conduct in society” (Reitz, 2004).

The study of the moral issues that result from the accessibility, accuracy, and availability of information resources are integral to Floridi’s (2006) Information Ethics (IE) model. The IE model’s components of accessibility, accuracy, and availability share commonality to a well-known IS security model, the CIA Triad, also referred to as the CIA Triangle (Figure 1). This popular security model is considered an industry standard by IS security professionals and is used as a basis for implementing security on information systems by identifying problems or weaknesses and establishing the appropriate security solutions. One of the most respected professional security certifications, the Certified Information System Security Professional (CISSP), uses the CIA Triangle as its model for implementing IS security. The CISSP certification is recognized by the International Organization for Standardization (ISO) and the

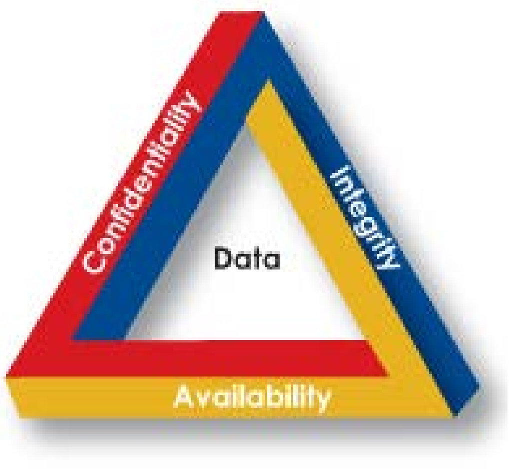


Figure 1: CIA Triangle

International Electrotechnical Commission (IEC) as an accredited information system security certificate and has been officially adopted by organizations such as the US Department of Defense (DOD) and National Security Agency (NSA) as an approved certification for their Information Assurance workforce (DOD 8570.01M). Researchers advocate that the key to effective security is based on the confidentiality, integrity, and availability (CIA) of the information system or the data maintained in it (Crook, Ince, Lin, & Nuseibeh, 2002; Evans, Heinbuch, Kyle, Piorkowski, J., & Wallener, 2004). Maintaining CIA is defined as information security according to the Information Security Management Standard ISO/IEC 17799 (Saint-Germain, 2005). Database security breaches are categorized as unauthorized exposure of data, incorrect data modification, and unavailability data (Bertino & Sandhu, 2005) which also aligns with the three components of the CIA Triangle.

The need for investigating the influences on the ethical decision making processes in regards to compliance with IS organizational security policies and processes was identified by Myyry et al. (2009). However, despite the significant role of human behavior on systems and the recognized applicability of ethics to IS security, the importance of ethics has been ignored or minimalized by most practitioners and researchers. Standardized models which provide a clear understanding of risks and incorporate the best methods of addressing risks within an organizational security plan, assess risk exposure, and provide processes to protect an information system such as described by Jones (2007) or Ketel (2008) do not mention the role of ethics. And ISO 17799, which is regarded as one of the primary and relevant standards regarding information system security (Ma & Pearson, 2005) does not consider the role and effect of employee ethics. Ethics in general and especially ethics based in philosophy has very little research tradition in the field of ISS (Adam & Bull, 2008).

2.5 Virtue Ethics is Important to Information System Security

Because IS workers are faced with moral decisions, IS ethics includes consideration of social and personal policies regarding the ethical use of computers (Moor, 1985). One of the essential factors for ISS management is realizing that one of the dimensions of ISS is ethics (von Solms & von Solms, 2004). ISS should be addressed from more than just a technical aspect; it needs to consider human issues such as culture, ethics, and training

(Eloff & Eloff, 2003). Siponen and Iivari (2006) recommend that that virtue theory should influence the application of ISS and that virtue ethics can help guide the application of security policies and guidelines.

Virtue ethics has previously been neglected, thought of as antiquated, and not considered suitable for use in Information Technology focused organizations (Stamatellos, 2011a); however in foundational research in computer ethics Artz (1994) argued that virtue ethics is the superior choice for computer ethics because of the types of choices IS users are presented with. Moor (1998b) also made a case for virtue ethics being applicable to IS ethics gaps and shortcomings. More recently studies by Adam and Bull (2008), Dahlsgaard et al. (2005), Drover, Franczak, and Beltramini (2012), and Stamatellos support the idea that virtue ethics is relevant to computer ethics because moral principles help users to make correct decisions about how to act on ethical problems presented during IS use. And while there are several forms of virtue ethics, computer ethicists generally emphasize the Aristotelian form (Stamatellos, 2011a).

Grodzinsky (2001) argues that ethical theories that are directed towards character formation and development such as virtue ethics are more applicable to IS ethics than action guided theories such as utilitarianism or deontology, both of which focus on what a moral agent should do in a situation without requiring that individual to internalize ethics. In contrast, the focus of virtue ethics is on being rather than doing, with any actions or choices made being internally initiated from the individuals self. The principles of virtue ethics focuses on the voluntary observance of right conduct and moral law rather than conforming to rules in order to obtain rewards or escape sanctions. Mandating morality through rules may not be adequate because rules typically have a negative nature in that they tell individuals what not to do. A moral principle approach is more desirable because the concepts of right and wrong are accepted by members of the group. Because this will result in goodness, Hart (2001) and more recently Stamatelleos maintain that organizations should strive to be principle vice rule oriented in their approach to developing virtuous character in its employees and culture.

Human behavior and organizational culture are crucial factors in protecting information assets and addressing ISS (Hilton, 2000; Vroom & von Solms, 2004). It is felt that behavioral security is vital to ISS success (Dhillon, Tejay, & Hong, 2007) and that employee attitudes and beliefs have a significant impact on whether they will comply with ISS policies (Pahnila et al., 2007). Self-governance and self-determination are components of virtue ethics that are applicable to cyber ethics and handling of information (Stamatellos, 2011b) and could be viewed as motivational approaches. However, it was noted early on that a significant challenge to the utilization of virtue ethics is that most managers are more comfortable using situational ethics to achieve organizational goals (Hart, 2001). In over 90% of organizations at least one serious IS violation occurs every year, with the majority being caused by individuals violating organizational security policies. Moral reasoning theories such as virtue ethics are applicable to ISS because employee decisions to violate policy are a result of moral conflict (Myyry et al., 2009). In 2000 Siponen recommended that organizations should find ways for employees to internalize the importance of complying with ISS policies because compliance motivations enforced by punishment are not as effective. They are also resource intensive because for punishment to work individuals have to believe that they will be caught; therefore monitoring efforts by the organization are required. Based on the numerous recent well publicized IS security breaches by trusted insiders these issues remain just as valid today.

Defining the ethical use of information systems is seen by many as a responsibility of an organization’s management (Hilton, 2000; Huff, Barnard, & Frey, 2008b) but an individual’s character, shaped by virtue ethics, can determine whether they will actually comply. Because culture and personal beliefs are important influencers on security behaviors, understanding an employee’s beliefs is critical (Alfawaz, Nelson, & Mohannak, 2010). Since so many security failures are rooted in employee behavior, research into socio-organizational factors can contribute to improving ISS (Hu et al., 2007). IS technological advances are occurring at a rapid pace, but the evolution of ethics in respect to the use of information systems is lagging behind (Dorantes et al., 2006). According to Grodzinsky (2001) in order for researchers to address or analyze the larger, more substantial ethical problems created by the incorporation of IT beyond just a theoretical level the individual issues surrounding moral agents must be examined. Deeper insight into ethical decision making is needed in order to protect these systems. Taking that into consideration, the use of virtue ethics can help to address the changing nature of ISS because it is based on developing enduring character traits in the individual making the ethical choice. Past research indicates that virtue ethics is an appropriate model for the development of personal ethics and character which in turn will carry into that individual’s professional ethics (Grodzinsky, 2001; Harris, 2008); however, there is very little research which explores virtue ethics based ISS constructs. Despite the apparent support for virtue ethics by the researcher community, Adam and Bull (2008) note that there has been no previous research efforts to apply the concepts to address issues in IS.

2.6 Technical Controls, Formal Procedures, and Policies are Ineffective

Organizations devote the largest part of ISS efforts to various security technologies and tools, but researchers argue that security cannot be achieved solely by technical controls (Herath & Rao, 2009; Wiant, 2005). Technical approaches such as the use of firewalls, intrusion detection and prevention systems, secure configuration of IT assets, and physical security measures are limited in effectiveness against insider threats because those individuals likely have legitimate authorization to access the IS they intend to exploit (Kraemer et al., 2009; Zeadally, Yu, Jeong, & Liang, 2012). Various studies have determined that ISS is a socio-technical issue and that the weakest component of ISS is the human factor, in particular people's attitudes and behavior regarding security (Colwill, 2009; Dhillon & Backhouse, 2001; Hu et al., 2006; Vroom & von Solms, 2004). It is contended that ISS is primarily not a technical issue, but one of management or business, meaning that system security is a social or human issue and because of this there are significant security issues which technical controls cannot address (Chang & Ho; 2006; Dhillon & Backhouse, 2000). This position is supported by D'Arcy and Hovav (2009) who state that technical controls which serve as a deterrent to some people are ineffective against others. However, most practitioners and researchers continue to focus on solutions to technical issues. Dunkerley and Tejay (2011) point out that technical controls have dominated research in the ISS field and that those technical controls have focused on ensuring the confidentiality, integrity, and availability of the information system including the associated information and data. Department of Defense (DOD) initiatives to ensure confidentiality, integrity, and availability are considered to be the origins of ISS research, but it is currently contended that an over reliance on this perspective limits the ability to understand, manage, and ensure IS security (Dhillon & Torkzadeh, 2006). When considering insider threats, an over dependence on technical controls for protection without considering other factors can result in significant failures in security (Colwill, 2009; Kraemer et al., 2009).

Backhouse and Dhillon (1996) claim that technical controls such as checklists focus on procedural details, but do not address what is really key – an understanding of the theoretical foundations of IS security. They advocate that past ISS risk analysis has found that people's behavior is one of the major factors in system security. Baskerville (1991) takes an opposing view, that the best approach to security implementation should be that it is incorporated into the systems design, but concedes that relying solely on a secure IS design to maintain system security could have negative consequences. While both studies are somewhat dated it remains that a case can be made for both approaches. And what is not disputed is that relying on technical controls to solve the majority of IS security issues were then and continues to be viewed as an ineffective solution (Colwill, 2009; Kraemer et al., 2009). While acknowledging the importance of technical controls and recommending that a holistic methodology which integrates technical and human related security controls and procedures into a system, it is posited by Eloff and Eloff (2003) that information security management should approach security issues from the human or social aspect in order to address security culture and ethics issues. According to Lim, Chang, Maynard, and Ahmad (2009) an organization's senior management must realize that technical and physical controls alone will not ensure IS security. Non-technical activities are accepted as being a part of Information Security Management (Herath, Herath, & Bremser, 2010; von Solms, 2005) and offer an alternative to the approach of relying solely on technical solutions. ISS non-technical activities include development of policies, procedures, training, and awareness programs; and conducting background checks on potential IS employees who will occupy trusted positions. However, Siponen et al. (2010) state that policies alone are not a deterrent against internal threats; while Workman and Gathegi (2007) and Grodzinsky (2001) assert that formal policies and procedures are meaningless if the persons they are directed at are insensitive to ethical matters. The conclusion drawn is that for any security solution to be effective it must also address the human perspective.

The Backhouse and Dhillon (1996) approach of associating technical problems within a social and organizational context allows for the integration of technical issues into the ISS norms of an organization. One common method of enforcing those norms and for preventing information systems risk is the General Deterrence Theory (GDT) (Straub & Welke, 1998) which supposes that the threat of punishment will deter or discourage a person from performing an undesired act, and that public knowledge of that punishment will also deter other individuals from performing similar undesired acts in the future. This visible punishment should lower IS abuse by convincing employees of the certainty of being caught and the associated severity of punishment (Straub, 1990; Straub & Welke, 1998). The GDT concept of perceived severity of sanctions and awareness of security policies has been found by D’Arcy, Hovav, and Galletta (2009) to improve IS security and they contend that the study confirms applicability and effectiveness of the

GDT to the ISS domain. Kankanhalli, Teo, Tan, and Wei (2003) also found that increased deterrence efforts result in improved effectiveness of IS security. Herath and Rao (2009), Straub and Welke (1998), Theoharidou et al. (2005) further endorse the application of GDT techniques such as disincentives and sanctions to mitigate or prevent IS abuse, but note that some researchers dislike GDT's negative aspects of monitoring and punishment of employees.

Other criticisms of GDT are that punishment has been shown to be primarily effective in dissuading only lesser motivated potential offenders, it is not as effective on highly motivated offenders (Wiant, 2005), and that proof of effectiveness in IS security is inconsistent (D'Arcy & Herath, 2011; Straub, 1990). It is clear that while the GDT has had some measure of success, in many instances deterrence is not effective in preventing violations. Additionally, regardless of the presumed effectiveness of the GDT many managers do not use deterrence to enforce IS security because they are not comfortable using the perceived negative aspects of punishment to address human behavior or they are not familiar with detection measures and preventative countermeasures (Straub & Welke, 1998).

As noted by Dhillon, Tejay, and Hong (2007), ethicality involves compliance with ethics codes and ethical work practices. Codes of ethics are written statements of policy that define appropriate standards of behavior by workers in regards to conduct and are increasingly being adopted by businesses to deal with crime, corruption, and abuses by employees. Over 80% of business organizations in the United States have codes of ethics in place (Harrington, 1996; Singh, 2011). These codes can help guide employees to find the best solution or choices when they are faced with ethical issues or dilemmas (Adams, Tashchian & Shore, 2001). Backhouse and Dhillon (1996) believe that in the majority of instances responsible employees will make decisions that conform to subjective norms such as an ethical code, and that the biggest issue to be concerned with from a security standpoint is that these norms are designed or written reflect the desires of the organization as well as any standard work practices, policies, statutory requirements, or professional codes. This viewpoint relies on effective norms and codes being in place, and for ethical people to follow them. It does not address the instances where the codes may be weak or that employees may for whatever reason, act unethically. Prior research supports the belief that ethics codes can deter undesirable behavior or actions by employees (Chun-Chang, 2007) and encourage what people ought to do (Wu, Rogerson, & Fairweather, 2001). However, while acknowledging that they do have some degree of positive impact on employee intentions, Harrington (1996) and Singh (2011) found that both general and IS specific ethics codes are generally weak and sporadic in preventing violations and controlling employee behavior; attributing this perhaps to the low probability of the employee being caught. Webley and Werner (2008) submit that ethics policies based entirely on organizational codes of ethics are inadequate for having an effect on behavior. This viewpoint is supported by many researchers who question the effectiveness and value of codes and policies; with many believing that there is minimal evidence of increased ethical behavior and they are in fact often counterproductive (Huff et al., 2008b; Kaptein & Schwartz, 2008). Harris (2008) notes that the effectiveness of ethics codes, policies, and other rules are limited because every situation cannot be captured, and that they do not address an individual’s internal motivations. Despite the lack of compliance and in spite of their apparent ineffectiveness, codes and polices do act as a guideline for desirable behavior, serving as a basis for an organization to use to take legal action against violators (Siponen & Vance, 2010). Even with these shortcomings, security policies and procedures are considered essential components for the effective protection and management of an information system (Karyda, Kiountouzis, & Kokolakis, 2005) and the approach recommended by security specialists for addressing misuse of an IS by organizational employees is through a mixture of technical controls, policies, and procedures (D'Arcy & Hovav, 2009).

Leonard, Cronan, and Kreie (2004) posit that a variety of factors including personal values and beliefs influence ethical actions and the effectiveness of professional policies such as codes of ethics. It is recognized that increased attention must be placed on the part played by organizational culture and the human element because the primary factor in ISS is people (Wiant, 2005). Regardless of which approach is taken, a review of legal requirements as mandated by applicable laws, regulations and directives is necessary for the identification of information protection requirements and system risks. This will help to identify and ensure compliance with appropriate controls while instilling in stakeholders a sense of confidence that the IS and its associated data, which is the most important asset, are adequately protected and managed (Gerber & von Solms, 2008).

Despite the research showing that technical controls, formal polices, and procedures alone fail to adequately protect an ISS, the number of research efforts focusing on management, social, and human concerns are few in comparison to those focusing on technical issues (Chang & Ho, 2006). Because the insider threat involves organizational, psychological, and psychosocial aspects attempting to address it from a strictly technical perspective is inefficient (Zeadally et al., 2012).

2.7 Information System Violations by Trusted Workers

Security violations by trusted workers who have access to organizational IS assets are a significant threat. These threats include the inadvertent loss or exposure of data and deliberate disregard for security or theft of information for personal gain or other motivations (Alfawaz et al., 2010). A 2009 study of information system data breaches found that 48% were conducted by organizational insiders (Zeadally et al., 2012). Not all ISS compromises by insiders are intentional, in fact many are accidental; however, the confidentiality, integrity, or availability of the information is still compromised (Colwill, 2009). Organizational security efforts historically focus on external threats or in response to legal or regulatory requirements or mandates (Jabbour & Menascé, 2009; Wiant, 2005). However, insider threats, those from IS workers in trusted positions, can be the most damaging and costly to an organization (Greenemeier & Gaudin, 2007; Kraemer, Carayon, & Clem, 2009). Insiders have the capability of causing more damage than outside attackers because they know which organizational assets are valuable, their location, know when the best opportunities are to attack, and likely know how to hide the evidence of their violation (Colwill, 2009). The significance of internal threats is becoming increasingly more apparent to IT executives (Wiant, 2005). Many managers and security professionals state that the insider threat is what they are the most concerned with because IS workers are placed in trusted positions, know what data is important or sensitive, and have access as well as the technical knowledge to exploit the system’s security controls (Greenemeier & Gaudin, 2007). The threat is not new, in 2001 Dhillon noted that while ISS is mainly implemented and managed by technical controls, those controls are ineffective against violations committed by trusted workers, who he identified as having emerged as the primary ISS concern. Trusted IS workers account for well over 50% of computer crimes with most violations being committed by employees who have intentionally bypassed or subverted security controls. Greitzer and Hohimer (2011) note that presently there is no effective approach to addressing the issue of insider attacks and that current practices are reactive and primarily forensic in nature, consisting mainly of monitoring, analyzing, and correlating data to detect the threat. The conclusion is that the rewards for committing computer crimes and unethical behavior appear to be greater than the risk of being caught (Balsmeier, & Kelly, 1996; Colwell, 2009).

Organizations typically conduct security or background checks of potential IT and IS employees, particularly those being hired for trusted positions. Those investigations look into a person’s criminal record, finances, foreign travel, and personal habits such as gambling and drug or alcohol use so as to identify whether the individual is a possible security risk. If the person does not have any red flags in these areas they are likely to be granted privileged access to sensitive or classified information. This methodology of vetting personnel for trusted insider positions has failed in numerous instances, most recently in the cases of Edward Snowden, Bradley Manning, and Robert Hanssen.

Research indicates that over 90% of IS security controls are implemented for protection against external attacks but that many attacks, including over 70% of fraud incidents, are committed by insiders. As pointed out by preceding research most technical controls are ineffective in preventing willful employee misconduct. Developing and implementing security frameworks which expand on conventional security approaches is essential for managing and mitigating insider threats to information systems, while trusting that an organization’s employees will be motivated by ethics (Jabbour &

Menascé, 2009). Greenberg (2002) researched the problem of worker theft from their employers and reached two conclusions; that employees with lower moral development committed more violations and that organizational ethics programs are less effective for those types of individuals. Despite the significance and potentially grave consequences to an organization presented by the trusted insider threat, a majority of CSOs are more concerned with externally initiated attacks (Colwill, 2009).

Rather than observing an employee's ethical behavior after they are hired and determining that they are not a good fit within the organization, identifying employees with good ethical principles prior to hiring them appears to be key to preventing ISS violations by trusted insiders. The challenge for organizations is to understand employee perceptions and motivations (Boss et al., 2009). Insiders commit violations because of their behavioral and motivational beliefs, therefore identifying those beliefs and changing them is also a potential solution to influencing workers not to commit ethical violations (Dhillon, 2001; Warkentin & Willison, 2009). Additionally, it has been noted (Andreoli & Lefkowitz, 2009; Dhillon & Silva, 2001) that organizational culture has a significant effect on whether employees will commit violations and that an organizational climate should be developed and fostered which encourages employee integrity as well as them being responsible for their actions. The payback to the organization is the reduction of risk from loss or compromise of data as past investigations into IS risk analysis have shown that a central component of ISS is people's behavior (Backhouse & Dhillon, 1996; Colwell, 2009). Moor (1998a) is more direct, stating that ethical points of view are necessary for achieving ethical responsibility. Accountability and responsibility are required for persons in positions of power (Grodzinsky, 2001) and trusted workers, particularly executives and senior management, are in positions of power over the operation and management information systems and ISS. Their support is critical to information security success (Hu et al., 2007; Thong, Yap, & Raman, 1996).

2.8 Summary

Analysis and synthesis of relevant literature was conducted to describe the theoretical perspectives and discover what is currently known and unknown about the role of ethics in information system security. It was found that violations by trusted workers who have access to information systems assets are a significant threat to security. The literature emphasized the importance of virtue ethics and their effect on the actions of IS trusted workers and details the many factors that influence an individual's decision making, including locus of control, ego strength, field dependence, feelings of responsibility, and organizational culture. All decisions made by people are influenced and driven by ethics (Donner, 2003). Ethics codes are part of organizational culture, but do not prevent ethics violations (Harrington, 1996; Webley & Werner, 2008). While somewhat effective in certain ISS studies, the General Deterrence Theory has been shown to not always be a reliable predictor or controller of human behavior (Wiant, 2005). Management support is critical to the success of ISS (Hu et al., 2007; Thong et al., 1996). Ethical choices are considered part of the systems development process and individuals are a component of ISS (Iivari, 1991, 2007); however, people's ethical actions are not always consistent (Banerjee et al., 1998). Research shows that a potential deterrent of IS ethical violations could be the identification of individual and situational characteristics (Banerjee et al., 1998; Haines & Leonard, 2007).

There is a need for better understanding of virtue within organizations (Dyck & Wong, 2010) and further investigation is needed to determine how the use of ethics and particularly virtue ethics could be an effective approach to addressing the ethical behavior of IS trusted workers (Myyry et al., 2009). While there is significant prior research in regards to ethics, most studies point to the importance of incorporating, implementing or enforcement of desired ethical conduct via corporate polices or codes. Additionally, while the use of information technology is now common place in the working environment, the development of the ethics that guide its usage lags far behind, therefore it is important to understand why employees act unethically in an IT context (Dorantes et al., 2006). Adam and Bull (2008) point out that ethics and ethical frameworks in IS use remains underexplored with no known research efforts having been conducted regarding the utilization of virtue ethics concepts in information systems. Colwill (2009) notes that a greater focus on human factors is needed to address insider threats by building organizational cultural values and citizenship and he recommends a focus on measuring and changing employee behavior through organizational development programs such as targeted training. According to Grodzinsky (2001) and Whetstone (2003) individuals interpret situations based on their background and experiences, therefore ascertaining details about moral agent’s ethical viewpoints are important to predicting how they may react in ethical situations. This knowledge plus the incorporation of virtue ethics concepts based on developing enduring character traits into training programs for employees may have the potential to address some of the challenges to ISS by insider threats.

As shown in the literature review, while the consensus is that virtue ethics can significantly effect and guide employee decision making and behavior and is an appropriate choice to improve ISS; the gap in the research is that very few studies have focused on how senior management can use virtue ethics to influence the ethical actions and choices of trusted workers in order to positively to effect ISS climate and culture or which identify or explore the concepts of virtue ethics based ISS constructs.

Chapter 3

Methodology

3.1 Introduction

This chapter describes how the research study was performed, presenting the theoretical basis, model, research questions, hypotheses, research methodology, data collection, analysis strategies, and resource requirements.

Social sciences are the studies of society, social activity, social and human behavior, and the relationship between individuals and groups. It consists of several disciplines including economics, politics, culture, and ethics (Gerber & von Solms, 2005). Gerber and von Solms point out that one of the more noticeable differences between social and natural sciences are that the natural sciences are concerned with objectively measurable observations, while the social sciences deal with subjective social and human behavior. As noted by Gerber and von Solms, while risks to information technology assets are real, social scientists evaluate them by subjective perceptions that are based on beliefs, opinions, and values. Additionally, it is being increasingly recognized that human behavior, the meanings associated with an individual’s actions, and an understanding of social interactions are important (Colwell, 2009).

In information system security (ISS) research the approach traditionally has been founded in positivism, one of understanding and verifying how events occur by using the scientific method, utilizing empirical data. In a study of IS research from 1991 to 2001, Chen and Hirschheim (2004) found that 81% of papers used a positivist approach versus 19% that used interpretive because the positivist methodology approach provides for a rational, formal analysis and design of an ISS. Alternately, it has been contended that looking at an ISS from an interpretive standpoint better enables researchers to understand an individual's actions and link them with a shared meaning of conduct (Dhillon and Backhouse, 2001; Lee & Hubona, 2009). Despite these contentions the positivist approach is the dominant method used in IS research.

Using the positivist approach this study endeavored to assess the content validity and reliability of four new virtue ethics based individual morality ISS constructs. It is contended that these new constructs collectively form the concept of ISS Virtue Ethics and through processes internal and external to the organization exert influence on the moral character of trusted information systems workers.

3.2 Theoretical Basis

The theoretical basis for this study was built upon the previous work and theoretical frameworks of Weber (1981, 1993) and Floridi (1999, 2006) in order to develop a new theoretical model for ISS trusted worker ethical behavior. Weber's research focuses on institutionalizing ethics into business organizations. According to Weber (1981, 1993, 2010) institutionalizing ethics consists of integrating ethics formally and explicitly into the day to day work practices and decisions of an organization's employees. He proposes a multi-component model for institutionalizing ethics into a business organization of which the components of Organizational Ethical Culture, Employee Ethics Training, Codes of Ethics, and Organizational Enforcement Mechanisms contribute to the desired result, specifically that of Employee Ethical Behavior.

Floridi (1999, 2006) researches the nature of Information Ethics, and has determined that existing theories of ethics are inadequate to address the ethical issues involving information systems. He describes his theory of Information Ethics (IE) as the study of moral issues that develop from information that a moral agent receives from an infosphere, defined as the environment in which information plays a significant role, such as an information system. Floridi (2006) describes the components of an infosphere as consisting of the:

- moral agent, the individual making the ethical choice or morally qualifiable action.
- info-resource, the information and its accessibility, accuracy, availability, and trustworthiness needed to make a decision.
- info-product, which is the result of a moral agents ethical evaluations and actions generated from information resources.
- info-target, how a moral agent's ethical evaluations and actions affect the infosphere and what it means to the rest of the information environment because of the moral agents actions and the resulting info-product.

Based on the work of Floridi (1999, 2006), the first assumption of this study was that an information system, the combination of Information Computing Technology (ICT) and human activities that support its operations, is considered an infosphere.

Floridi and Sanders (2005) are critical of the use of virtue ethics as a basis for cyber ethics in an information society, stating that virtue ethics is focused on ethical individualism and self-construction; and that it can be intolerant because people's basic beliefs often stem from their religious roots which may conflict with the beliefs of others in a global society. It is important to note that the context of Floridi and Sanders research was specifically in regards to the use of the Internet, not by moral agents filling the role of IS workers. Floridi and Sanders believe that because of its individualistic nature virtue ethics is not appropriate for use in globalized societies such as the Internet where the focus is on global values, contending that by using virtue ethics a moral agent will attempt to use their own ethical principles to address global ethical issues, with undesirable or unintended global consequences. Floridi and Sanders point is that because virtue ethics focuses on individual development it is unsuitable for use in virtual communities or information societies such as the Internet where any decisions that may affect that entire community are disregarded. However, numerous researchers disagree, finding that a virtue based framework is appropriate for use in information systems, which is what the Internet is (Adam & Bull, 2008; Artz, 1994; Grodzinsky, 2001; Siponen & Iivari, 2006; Stamatellos, 2011b). Hart (2001) points out that virtue ethics has always been characterized by moral obligations for a person to think and act beyond their own self interests. Finally, Aristotle (2005) states that the development of virtues must take into consideration that all humans are related.

The theory of IE claims that an individual's morals guide their decisions and behavior, and Floridi (2006) maintains that although IE is a secular approach to addressing moral issues it is compatible with and may even be associated with Christian concepts of morality such as those espoused by Aquinas (2005) in his treatise on virtue ethics. While IE does not address individual ethical issues themselves its concepts can be used to develop or shape a conceptual framework which will lead moral agents to solutions to specific problems (Floridi, 1999; Floridi & Sanders, 2002).

Ethics are rooted in philosophy and understanding; and defining ethical behavior is key to the process of institutionalizing ethics (Weber, 1993). The Greek philosopher Socrates, who was noted in Western civilization for his contributions to the foundation and study of ethics, argued that the more information a person had regarding an ethical choice then the more likely it would be that the person would make the correct choice. Floridi (2006) however, disagrees, stating that more and better information does not necessarily lead to more ethical actions. This supports the contention that virtue ethics can play a role in ethical decision making because regardless of the amount of information the individual has or does not have, the virtue ethics theory advocates that an individual will do the right thing because they have internalized that it is in fact the right thing to do. A noteworthy point made by Floridi (1999) and Floridi and Sanders (2002) are that actions taken by a moral agent which contribute positively to the welfare of an infosphere are considered to be virtuous.

The literature review conducted in Chapter 2 of this study suggested notable findings regarding the importance of ethics from IS security researchers that can readily be presented within the framework of Floridi (2006). Information Ethics has been established as a distinct, separate research area and it is expected that in the future it will develop relationships with other ethical theories. It is also recognized by the research community that Floridi has contributed significantly to the development of Information Ethics (Dodig-Crnkoviv & Hofkirchner, 2011; Ess, 2008). However, Floridi’s work is not without critics. Siponen (2004) takes issue with Floridi’s concept that any information entities, including non-human objects such as computer software have moral claims, stating that for the entity to be a morally responsible agent one has to be able to hold discussions with it. Obviously this is not possible with non-human objects. Despite his criticism of certain aspects of the theory, Siponen does not find the IE Theory or the IE Model fundamentally flawed. While the remainder of Floridi’s theory which extends ethics beyond humans was not considered in this study, the IE model he presents appears to represent a valid viewpoint of Information Ethics. Based on the literature review the second assumption of this study was that Floridi’s (1999, 2006) IE model has been accepted by the research community as a valid ethical model.

In the context of ISS, virtue ethics has the potential to affect trusted worker ethical behavior and ultimately system security by providing a means of identifying existing character traits as well as a methodology to follow for developing and/or influencing desired traits which may predict or foresee how an employee will respond when presented with an ethical situation. With the understanding that trusted workers have privileged or elevated access to system information and knowledge of how to circumvent system security controls or conceal illegal actions, an ethical methodology that appeals to the internal motivations of an individual has the potential to provide more effective protection of system information.

3.3 Research Model

According to Moor (1985) a significant portion of computer ethics research is comprised of developing conceptual frameworks for understanding ethical issues involving computer technology. Adam and Bull (2008) note the need to explore alternate ethical frameworks such as virtue ethics in order to address IS issues. Whetstone (2001, 2003, 2005) determined that virtues are essential moral attributes required of organizations and people, that virtue based frameworks may be a method for management to develop an organizational ethical culture, and that there is a need to determine which constructs and characteristics are applicable to the organizations mission.

The potential positive impact of virtue ethics on the ethical behavior of trusted workers and the subsequent effect on IS security indicated a need to integrate the phenomena into a new security model. The research in this study integrated and expanded upon elements of the Multi-component Model to Institutionalize Ethics into Business Organizations, Figure 2, as proposed by Weber (1993) which focuses on organizational influences; and the Internal Resource Product Target (RPT) Information Ethics Model presented by Floridi (1999, 2006) and Floridi and Sanders (2002) as shown in Figure 3, which considers various influences and their presence or absence which effect the actions of moral agents. The RPT model helps to frame issues and interpretations of IE by focusing on information itself rather than on specific technologies; however, by Floridi’s (2006) own admission the model is over simplified and is not sufficiently inclusive of other factors such as addressing certain issues or factors which do not fall in any of the infosphere areas. It is also important to note that Floridi’s info-resource dimension only addresses information and its quality, and specifically only information which is contained within the infosphere. Based on Floridi’s admission of those shortcomings it is proposed that the addition of an influencers’ dimension, or info-influencer, as a variable that acts upon the development of the ethicality of people be incorporated into his RPT model.

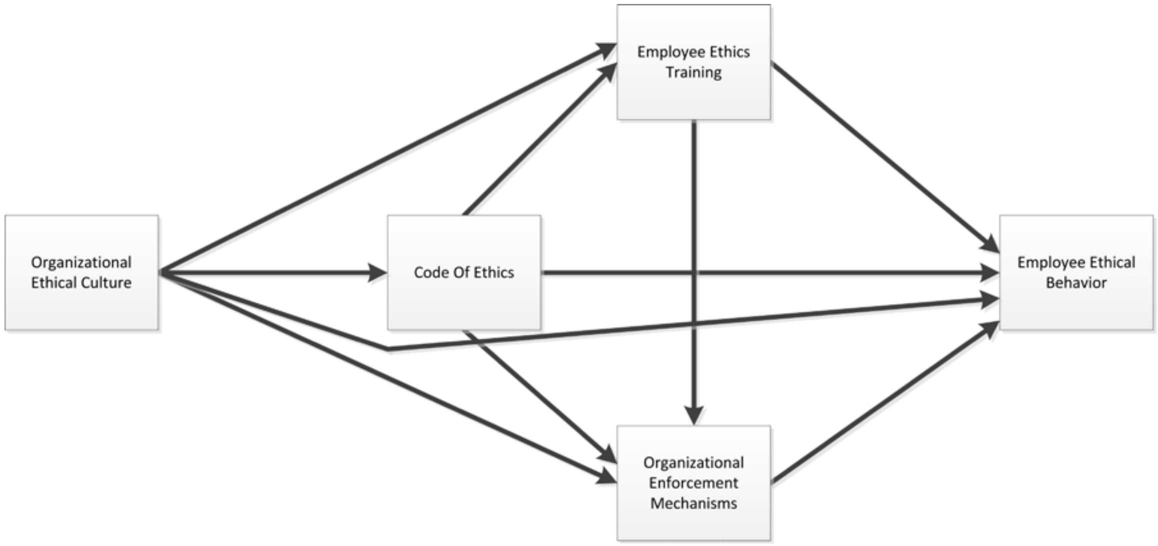

Employee Ethics Training
Organizational Ethical Culture
Code Of Ethics
Employee Ethical Behavior
Organizational Enforcement Mechanisms

Figure 2: Multi-component Model to Institutionalize Ethics into Business Organizations

From "Institutionalizing Ethics into Business Organizations: A Model and Research Agenda," by J. Weber, 1993, Business Ethics Quarterly, 3(4), p. 420. Copyright 1993 by Business Ethics Quarterly. Reprinted with permission.

This Revised RPT Information Ethics Model is shown in Figure 4. The info-influencer dimension is comprised of internal and external influences which contribute to the development and make-up of a moral agent's personal ethics. A moral agent, represented by the box labeled "A" in Figure 4, is effected by, brings into, or draws on these info-influencers when making decisions.

The third underlying assumption of this study was that the factors that shape a moral agent's moral and ethical deliberations are not identified or included as part of Floridi's (1999, 2006) infosphere, the information system. As illustrated in Figure 4, these influences can originate from either inside or outside the infosphere. The presence or absence of these influencers effects the actions of people and ultimately the security of an IS.

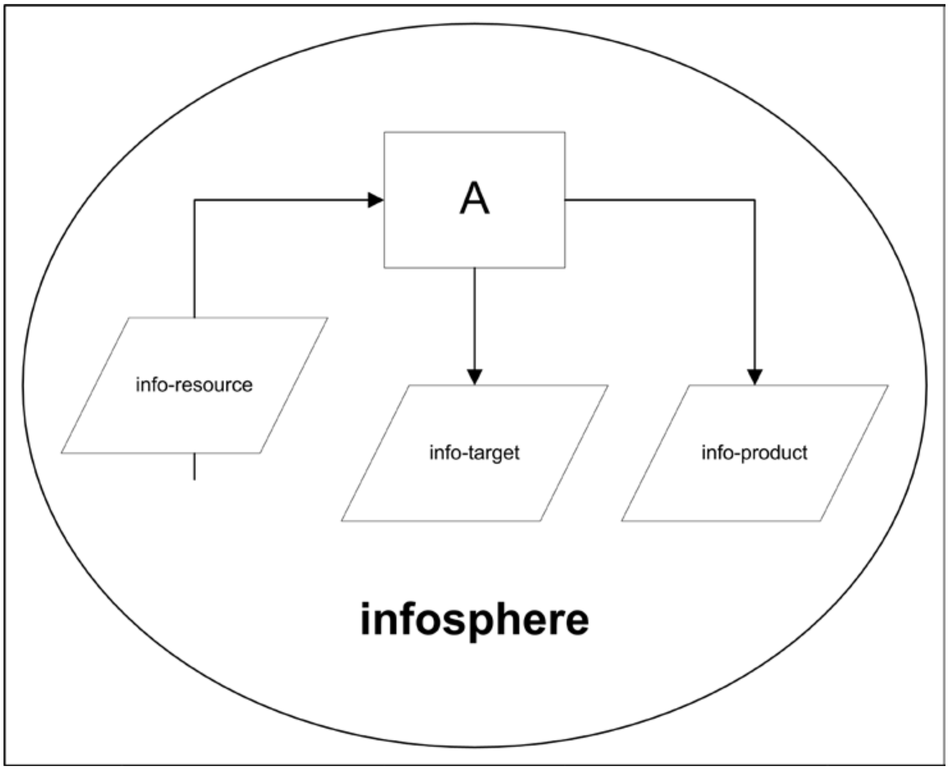


Figure 3: RPT Information Ethics Model

From “Information Ethics, its Nature and Scope,” by L. Floridi, 2006, Computers and Society, 36(3), p. 24. Copyright 2006 by SIGCAS Computers and Society. Reprinted with permission.

An important internal influence is whether the moral agent feels that the organization that has authority within the infosphere is conducting and directing actions that are morally correct. Therefore the forth assumption of this study was that the authoritative organization is acting morally – doing the right thing.

While many virtue ethics studies such as Artz (1994), Chun (2005), Harris (2008), Shanahan and Hyman (2003), and Whetstone (2003) expand on the list of what are considered virtues, historically the virtues and virtue ethics are based on the four cardinal virtues as defined by Aristotle (2005) and Aquinas (2005). Those cardinal virtues; the constructs of temperance, fortitude, prudence, and justice; and their characteristics are described in the literature review in Chapter 2. Previous researchers have identified or proposed numerous other virtues such as faith, hope, and love (Dahlsgaard et al., 2005), empathy, piety, and respect (Shanahan & Hyman, 2003) and integrity, conscientiousness, and zeal (Chun, 2005); however, an assumption of this study was that the concept of virtue ethics is derived from the four cardinal virtues of temperance, fortitude, prudence, and justice as defined by Aristotle (2005) and Aquinas (2005). To the best of this

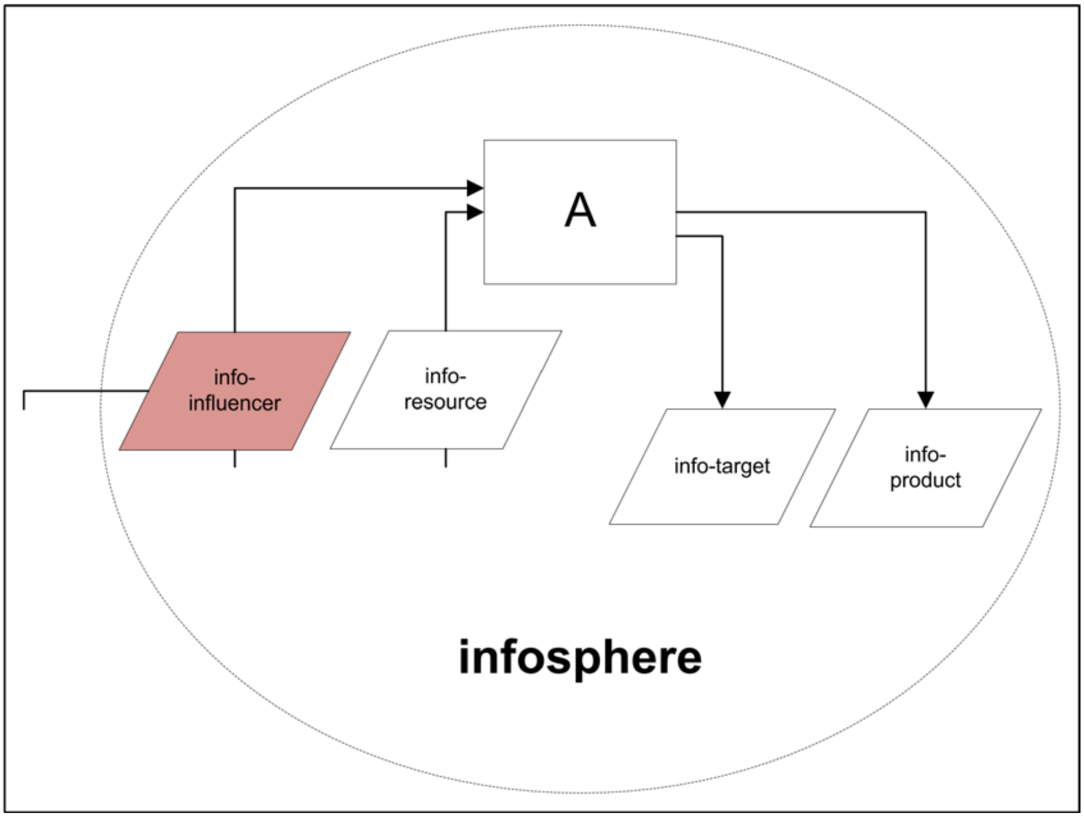


Figure 4: Revised RPT Information Ethics Model

Adapted from “Information Ethics, its Nature and Scope,” by L. Floridi, 2006, Computers and Society, 36(3), p. 24. Copyright 2006 by SIGCAS Computers and Society. Adapted with permission.

researcher’s knowledge what has not been defined by previous research is the identification, mapping, and validation of the concepts of virtue ethics to ISS formative constructs, particularly as they relate to IS trusted workers attitudes and behavior regarding ISS compliance.

While the previous references in this study refer to information systems workers in trusted positions, not all IS workers are actually employed in those types of positions. In this study IS workers who have role-based elevated privileges on the ICT are considered to be trusted workers. Also, because information systems security managers typically have the capability to affect the security posture of an information system through their decision making authority, technical knowledge and access to make system configuration changes, or by having elevated privileges that makes sensitive data available to them; they are generally also considered to be in trusted positions. Decisions made by trusted workers regarding configuration, operation, or management of the IS can affect the systems security posture, therefore the ethical actions of these individuals were the focus of this study.

According to Petter, Straub, and Rai (2007) constructs are abstractions used to describe and define a phenomenon of theoretical interest that may be observable - such as task performance, or unobservable - such as attitudes; and they can focus on behaviors, outcomes, or cognitive/psychological aspects of the item being investigated. Additionally, constructs are more general than specific behaviors. Freeze and Raschke (2011, p.3) state that the meaning of a construct is “conceptualized from theory and is represented within the researcher’s interpretational framework of the construct. A researcher’s challenge is transitioning from the theoretical meaning to the operationalization of the construct measure." A literature review provides the basis for the development of constructs (Petter et al., 2007; Roberts, 1999). Hinkin (1995) states that a validation of new construct measures or indicators begins with item generation, with the primary concern being content validity. Prior IS research has identified the personal and professional qualities of successful IS workers which contribute positively to desired security behaviors and organizational culture. The body of knowledge was reviewed to identify behavioral and ethical characteristics of ISS trusted workers that potentially correlate to the cardinal virtues as defined by Aristotle (2005) and Aquinas (2005). Based on the literature review the four information system security trusted worker ethical behavior constructs of Astuteness, Conviction, Rectitude, and Self-Discipline rooted in virtue ethics were proposed, potential indicators identified, and it was suggested how they may influence the character development and moral choices of information system security workers. The literature review also identified indicators of the virtue ethics constructs of Temperance, Fortitude, Prudence, and Justice and facilitated item generation of potential measures for each of the proposed formative constructs and their definitions as they relate to information system security.

The proposed construct of Astuteness aligns with the virtue of prudence or practical wisdom, characterized as a person being able to effectively deliberate and reason between actions with regard to which is appropriate at a given time. Stamatellos (2011a) advocates that ethical computer behavior is comprised of morally right actions, intellectual excellence, and responsibility. Myyry, Siponen, Pahnila, Vartiainen, and Vance (2009) found that compliance with IS policies and moral behavior is determined by an employee's skills, creativity, having a priority for moral values rather than other personal values, being able to recognize or interpret situations which involve moral issues, being motivated to act morally, and having an ability to rationalize the importance of IS security policies. An individual’s expertise, following best practices, and making impartial decisions during the design and deployment of information systems are ethical characteristics identified by Adam and Bull (2008). Numerous researchers have noted that employee professional skill, knowledge and awareness of security issues, and their abilities - particularly that of being able to conduct threat appraisals impact ISS (Alfawaz et al., 2010; Pahnila et al., 2007). Artz (1994) maintains that virtue ethics principles for computer systems includes wisdom and awareness of proper actions and use, while according to Alfawaz, et al. IS security behavior is affected by an individual’s knowledge, professional skills, and values coupled with consistent behavior. Virtuous acts include an individual being able to resolve conflicts between organizational goals and security policies according to Siponen and Iivari (2006). Finally, Siponen (2000) advocates that employee actions should be logical and consistent while recognizing any ethical issues as they pertain to ISS. Consideration of the cited research provides an aggregate definition of ISS Astuteness; skill in making assessments and in the application of professional knowledge, experience, understanding, common sense, or insight in regards to information system security.

Conviction is the proposed construct which is equivalent to the virtue of fortitude, also referred to as courage; recognized as the ability to confront fear, uncertainty, or intimidation. Alfawaz et al. (2010) maintain that possessing the clarity to understand and willingness to comply with and enforce security policies are behaviors which contribute to ISS. Stamatellos (2011a) states that computer use based on virtues requires the user to enact character based development which focuses on personal growth, improvement, and development of the moral self - the mental image a person has of themselves. Stamatellos (2011a, 2011b) notes that this is accomplished by an individual making self-determinations rather than choices expected by social norms, and that a virtuous person's instincts will tell them when their moral actions are good. Complying with ISS requirements requires certain moral behavior including that of making morally correct judgments, internalizing policies, and having the courage to follow right moral actions even when placed under pressure (Myyry et al., 2009). Regarding computer ethics based on the virtues, Artz (1994) points out that the burden of responsible actions is on the user, and that ethical use of the system will not have to be rationalized. A user intending to commit a violation may rationalize to themselves that committing the violation is the right choice, and sometimes it takes courage to make the ethical choice when it appears not to be beneficial to do so. Based on the literature cited a definition of ISS Conviction is that it consists of fixed or firmly held beliefs regarding information system security that affect decisions regarding compliance.

Rectitude is synonymous with the virtue of justice, which is concerned with acting fairly, responsibly, and being sensitive to the rights of others. Virtue based ISS work ethics are created by promoting loyalty, respect, and trust, particularly when safeguarding sensitive information (Dhillon & Torkzadeh, 2006). Alfawaz et al. (2010) concur that proper security behavior includes the IS worker being sensitive to the loss of system data. Rather than focusing solely on the loss of data, Myyry et al. (2009) take an organizational view by advocating that compliance with ISS requirements involves making morally fair judgments regarding security policies. According to Adam and Bull (2008) the ethical approach to using an IS includes treating coworkers, customers, and management well while striving to positively promote the employing organization. The opinion of Stamatellos (2011a) is all-encompassing in that cyber ethic morals and behavior includes feelings of caring, considerations of personal policies, social policies, and of making decisions that may affect society; with the aim of the moral agent to be that of achieving good netizenship – that of being aware of one’s civic responsibilities while participating and engaging with others in the Internet society, through character based morals. All of these concepts seem to appropriately align with the concept of ISS Rectitude, interpreted as the rightness or correctness of conduct and judgments that could affect information system security.

The virtue of temperance, defined as individual humility, self-restraint, and control of emotions and actions is represented in ISS by the construct of Self-Discipline. It is contended by Alfawaz et al. (2010) that an organizational culture that promotes ethical conduct will realize security compliant behaviors as employees will follow policies and rules, make rational decisions, and will perform rational actions in regards to ISS. Research by Pahnila et al. (2007) found that employee beliefs, conduct, habits, and having a positive attitude influences others within an organization and contributes to ISS. It is noted by Siponen (2000) that control of emotions are key to rational decision making by employees and contributes to their commitment to organizational information security. According to Stamatellos (2011a) an ethical and virtuous moral agent displays self-guidance and is self-centered in that they are subject to and in control of their own actions and decisions, and are therefore self-responsible. By doing so they have achieved a moral selfhood which contributes positively to ethical IS use. An individual’s work ethics are positively affected by improving their morals and professionalism, and one of the ways this is accomplished is by minimizing or controlling any temptations which may result in personal benefit, thereby contributing to the security of an information system (Dhillon & Torkzadeh, 2006). Myyry et al. (2009) state that a moral agent’s temptations to commit security violations are controlled by their own willpower and self-discipline. Willpower and control over one’s personal desires and conduct when considering actions that affect information system security sums up the primary concept of this proposed ISS construct.

The cardinal virtues, their aggregate definition as derived from the literature in Chapter 2 and the proposed ISS constructs and associated definitions based on indicators as identified by other researchers are summarized in Table 1, ISS Trusted Worker Ethical Behavior Constructs. In this study these virtue ethics based ISS constructs are incorporated into a theoretical framework for creating character measures for ISS trusted workers. The new theoretical constructs and their associated definitions are summarized in Table 2, ISS Theoretical Construct and Definition Summary. As noted by past researchers in the literature review in Chapter 2, virtue ethics principles can influence the ethical choices of moral agents. The reflective behaviors caused by the four new constructs have the potential to be used to affect trusted worker behavior through virtue ethics based character development. Introduction of this branch of ethics into the field of information systems security has the potential to contribute the identification of desired virtuous indicators and an examination of the factors that affect and shape the ethical perspectives of individuals entrusted with privileged access to personal, sensitive, or classified information maintained in an IS. An understanding of these factors can be used by organizations to influence trusted worker ethical intentions and commitment.

Table 1: ISS Trusted Worker Ethical Behavior Constructs

Cardinal Virtue	Definition	IS Security Construct and Definition	IS Security Construct Indicators	Reference
Prudence (Practical Wisdom)	A person’s considerations, judgments, and actions are based on knowledge, experience, and input from others and that they result in morally correct decisions.	Astuteness Skill in making assessments and in the application of professional knowledge, experience, understanding, common sense, or insight in regards to information system security.	Ethical computer behavior involves intellect, morally right decisions, and responsibility	Stamatellos (2011a)
			IS policy compliance is determined by skill, creativeness, priority for moral values over personal values, correctly interpreting situations as involving moral issues, being motivated to act morally and rationalizing importance of policies	Myyry, Siponen, Pahnila, Vartiainen, and Vance (2009)
			Performing job well, making impartial decisions	Adam and Bull (2008)
			ISS affected by a person’s knowledge, abilities, and professional skills	Pahnila, Siponen, and Mahmood (2007)
			Awareness of appropriate and correct use, wisdom	Artz (1994)
			Values, knowledge and skill affect ISS compliance. Consistent behavior is needed when addressing ISS issues	Alfawaz, Nelson, and Mohannak (2010)
			Ability to resolve conflicts between policies and organizational goals	Siponen and Iivari (2006)
			Recognition of ethical issues in regards to ISS, making logical decisions, consistent security actions	Siponen (2000)

Table 1: ISS Trusted Worker Ethical Behavior Constructs (continued)

Cardinal Virtue	Definition	IS Security Construct and Definition	IS Security Construct Indicators	Reference
Fortitude (Courage)	Personal integrity and willpower to make ethically correct or unpopular decisions despite pressures to do otherwise, even if it results in little or no personal benefit, risks loss of personal position, or creates adversity	Conviction Fixed or firmly held beliefs regarding information system security that affect decisions regarding compliance.	Computer ethics involves self-determination, how one should act in particular situations, character based development focusing on greater good over personal desires	Stamatellos (2011a, 2011b)
			IS policy compliance determined by courage, working under pressure, right judgments and willpower. Policy requirements are internalized	Myyry et al. (2009)
			Ethical use of IS does not have to be rationalized	Artz (1994)
			Understanding and willingness to comply with and enforce security	Alfawaz et al. (2010)

Table 1: ISS Trusted Worker Ethical Behavior Constructs (continued)

Cardinal Virtue	Definition	IS Security Construct and Definition	IS Security Construct Indicators	Reference
Justice	Being sensitive to the rights of others and acting fairly and responsibly towards individuals, organizations, and communities.	Rectitude Rightness/correctness of conduct and judgments that could affect information system security	Ethical computer behavior involves netizenship; a feeling of caring, consideration of personal and social policies, and decisions that may affect society	Stamatellos (2011a)
			IS policy compliance involves making fair judgments	Myyry et al. (2009)
			Ethical use of an IS is important to advancing an organization and treating colleagues well	Adam and Bull (2008)
			Being sensitive to loss of IS data	Alfawaz et al. (2010)
			Organizational loyalty and trust and respect for coworkers promotes security. Safeguarding sensitive information	Dhillon and Torkzadeh (2006)

Table 1: ISS Trusted Worker Ethical Behavior Constructs (continued)

Cardinal Virtue	Definition	IS Security Construct and Definition	IS Security Construct Indicators	Reference
Temperance	Self-restraint in conduct, humility, and self-control of emotions and actions.	Self-Discipline Willpower and control over one's personal desires and conduct when considering actions that affect information system security.	Ethical computer behavior involves self-guidance, moral self-hood, and being self-centered	Stamatellos (2011a)
			IS policy compliance is determined by self-discipline	Myyry et al. (2009)
			Attitudes and beliefs affect ISS compliance	Pahnila, Siponen, and Mahmood (2007)
			Willingness to follow rules and rational acts/decisions by employees contributes to security compliance	Alfawaz et al. (2010)
			Professionalism leads to ISS	Dhillon and Torkzadeh (2006)
			Ability to justify and have rational reasons for actions	Siponen (2000)

Research models propose relationships between the variables under study (Roberts, 1999). A new theoretical model, the ISS Trusted Worker Ethical Behavior Model (Figure 5), was proposed within an ISS virtue ethics domain. This model represents various entities or components, their attributes, and relationships within the domain; in particular that of demonstrating influences on ISS trusted worker behavior within an organization. The four cardinal vrtues of Temperance, Fortitude, Prudence, and Justice, redefined as ISS Self-Discipline, Conviction, Astuteness, and Rectitude respectively, form the core of the ISS Trusted Worker Ethical Behavior Model (TWEB). This research model builds upon the research and theoretical frameworks of Weber (1981, 1993) on institutionalizing ethics into organizations and Floridi (1999, 2006) on Information Ethics in informational

Table 2: ISS Theoretical Construct and Definition Summary

ISS Theoretical Construct	Construct Definition
ISS Astuteness	Skill in making assessments and in the application of professional knowledge, experience, understanding, common sense, or insight in regards to information system security
ISS Conviction	Fixed or firmly held beliefs regarding information system security that affect decisions regarding compliance
ISS Rectitude	Rightness or correctness of conduct and judgments that could affect information system security
ISS Self-Discipline	Willpower and control over one’s personal desires and conduct when considering actions that affect information system security

environments which he terms “info-spheres” but in the context of this research was referred to as an organization. It is important to note that all four constructs are required to adequately describe the concept of ISS Virtue Ethics, the main topic of this study. Although each ISS virtue ethics construct was measured to the trusted worker ethical behavior construct individually, in the model they are represented as one line in order to keep its concept clear.

The TWEB Model is comprised of seven components grouped into the three structural categories of Virtue Ethics, Influencers, and Effects. The definitions of these categories and their associated components are summarized in Table 3, TWEB Model Categories.

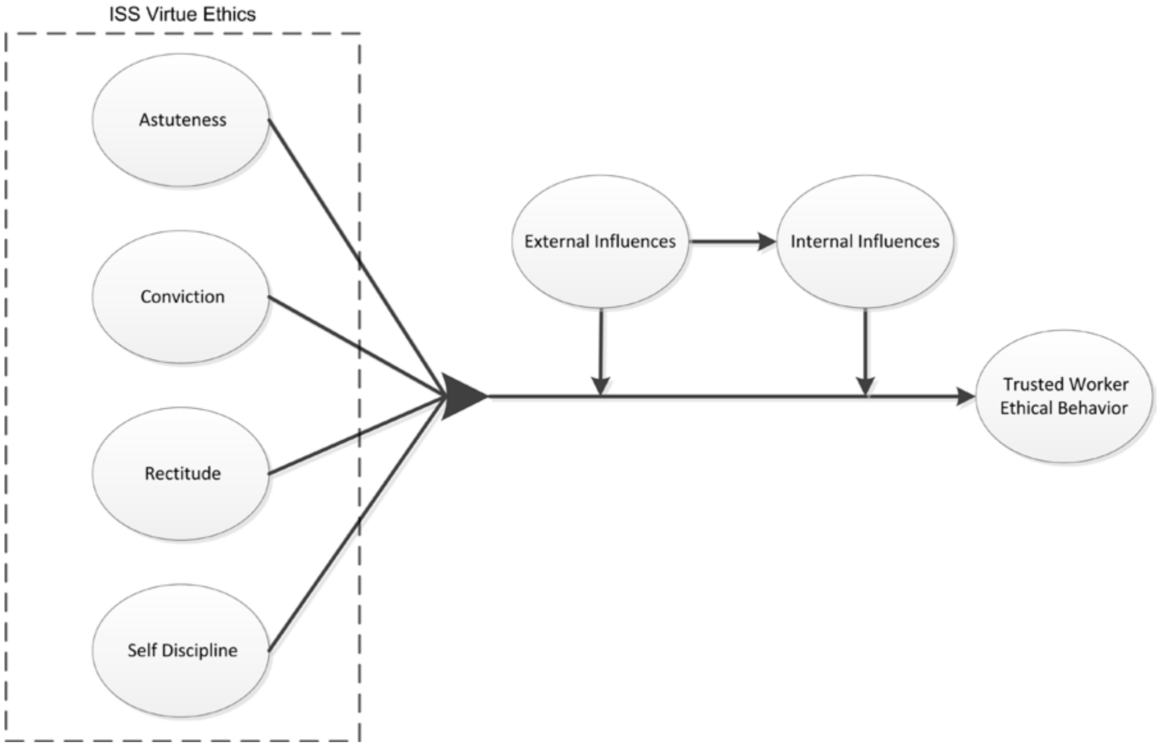


Figure 5: ISS Trusted Worker Ethical Behavior Model

The Virtue Ethics category is comprised of four ISS components; the constructs of Astuteness, Conviction, Rectitude, and Self-Discipline; derived from the cardinal virtues of Prudence, Fortitude, Justice, and Temperance respectively. These virtue ethics based ISS constructs form the basis of the proposed theoretical model. It is advanced that they shape the ethical beliefs, character development, and personal ethics of a moral agent which ultimately results in professional ethics. While developed as four individual constructs, for the sake of facilitating measurement and analysis they are considered sub-components of the multidimensional construct of ISS Virtue Ethics. As suggested by Mackenzie, Podsakoff, and Jarvis (2005) this should be done when multiple indicators and constructs are required to completely capture the concept of the domain. These four virtue ethics based constructs never solely or directly affect trusted worker ethical behavior; they are always filtered through influencers which moderate their effect.

Table 3: TWEB Model Categories

Category	Definition	Trusted Worker Ethical Behavior Model Component(s)
Virtue Ethics	Ethical concept that emphasizes the role of moral character and virtue in the character development and personal ethics of a moral agent	Astuteness, Conviction, Rectitude, and Self-Discipline
Influencers	Organizational and societal factors that impact or shape the ethical makeup, moral choices, and behavior of a moral agent	Internal and External Influences
Effects	Decisions and/or actions resulting from the influences on the moral considerations or a moral agent	Trusted Worker Ethical Behavior

The Influencers category of the TWEB model consists of environmental factors that are internal and external to the organization which exert a moderating influence on the ethical makeup, moral choices, and behavioral intentions of a moral agent. The Effects category indicates the outcome or consequence that the constructs and internal and external influences have on the resulting behavior of a moral agent, who in the context of this study is defined as trusted workers with privileged access to information systems.

The influencer components are comprised of internal and external influences and include factors such as age, education, intrinsic beliefs, religious institutions, peers, social organizations, training, and values. Influencers may impact the nature of the relationship between the independent and dependent variables (Sekaran & Bougie, 2010). They act as moderating variables that may produce an interaction effect in terms of direction or strength between the ISS constructs which are the independent variables, and any resulting trusted worker ethical behavior which is the dependent variable. The indicators of the moderating variables and the dependent variable of this study’s research model as well as the associated survey question are detailed in Appendix B.

An internal influence refers to any factor that is exerted from within an organization. Attempts to integrate ethics into an organization can occur through various business processes and organizational influences are recognized as important factors in moral development and ethical decision making (Singhapakdi, Vitell, Rallapalli, & Kraft, 1996; Trevino, 1986). The internal influencer component consists of the following five elements: organizational guidance, management behavior, enforcement sanctions, resource pressures, and work environment.

Researchers have developed several key organizational guidance influences on employee ethical decision making processes including ethics training, ethical codes of conduct, and ethics policies (Adler, 1983; Jackson, 2000; Tyler & Blader, 2005; Weber, 1981, 1993, 2010). Trevino (1986, 1990) and Weber (1981, 1993, 2010) state that one approach to ethical development and change is through employee orientation and training, and that organizational climate is an important factor in the moral development of an employee. Organizations develop ethical codes of conduct, ethics training, and ethics policies with the expectation of them having a positive impact on the ethical behavior of employees; and ethics training has been shown to be an effective method for moral development (Robertson & Fadil, 1999). Incorporating ethics training into managerial development programs as a discipline for decision making would promote efforts to institutionalize ethics into an organization (Weber, 1981, 2010). According to Weber (1993) ethics training is a key contributor to an organization's culture if ethics is to be integrated into employee conduct and actions, but he notes that the type of ethics training that is the most effective in influencing employee behavior is not known. Despite the uncertainty of which type best promotes the desired behavior, the majority of companies in the US conduct ethics training. However, Harrington (1991) states that the objective of ethics training is typically on employee decision making in order to avoid unethical behavior and noted that management has tended to be the primary recipients of this type of training.

Senior executives within an organization are also a significant influence on ethical standards through their decisions, actions, and because they are perceived as role models by employees (Brown, Trevino, & Harrison, 2005; Kaptein, 1998; Newstrom & Ruch, 1975; Trevino, Hartman, Brown, 2000). Additionally, Weber (1981) notes that management decisions and processes ultimately manifest themselves as character traits. Hu et al. (2007) found that ISS success is dependent upon upper management promoting awareness and the importance of information security.

Enforcement sanctions include organizational inducements such as rewards and punishment. Discipline serves as an important method of enforcement of ethical behavior and using it can determine the effectiveness of norms (Ball, Trevino, & Sims, 1994; Falkenberg & Herremans, 1995; Trevino, Weaver, Gibson, & Toffler, 1999). Resource pressures such as budget constraints, available equipment, personnel staffing, unrealistic performance expectations, and time or scheduling milestones that are placed on employees may affect their ethical decision making (Kaptein, 1998; Schweitzer, Ordóñez, & Douma, 2004; Trevino, 1986). The work environment; which consists of culture, morale level, presence of hostility or mistrust; can shape the ethical choices of workers (Hollinger & Clark, 1982; Kaptein, 1998; Skarlicki, Folger, & Tesluk, 1999). Each of these represents processes internal to an organization that potentially influence the ethical considerations of an individual and are included in the influencer component of the TWEB model. The model provides a framework to recognize these internal motivations and determine if it is feasible and effective to incorporate, either individually or collectively, the four proposed ISS constructs into the various internal processes of an organization in order to positively shape, guide, or influence the ethical evaluations, actions, and behavior of IS trusted workers.

Floridi (1999, 2006) concurs that influences on moral decision making can originate from within an organization as detailed by Weber (1981, 1993, 2010), but points out that they also originate from sources external to the organization. Floridi (2006) also states that an all-encompassing approach to Information Ethics must take into consideration all aspects of how information is created and used, and all entities involved that may interact with a moral agent. External influences on a moral agent's personal ethical values and behavior include their religious beliefs, cultural background, personal variables, social interactions, and personal relationships.

Throughout the world religious beliefs are a foundation for ethics in society and are the basis for how many individuals justify or view their ethical actions (Dahlsgaard et al., 2005; Floridi & Sanders, 2005; Keller et al., 2007; Shanahan & Hyman, 2003). As noted by Harris (2008) virtue ethics is an important aspect of religiosity, and religious based beliefs are appropriate and often used in organizations to determine the "goodness" of proposed actions (Cunningham, 1998). The effect of religiosity on shaping a moral agent's values and norms has been noted by numerous researchers and is a predictor of a person's ethical behavior (Keller et al., 2007; Parboteeah, Hoegl, & Cullen, 2008). Cultural background includes factors such as ethnicity, national heritage, traditions, and socioeconomic status, each of which establishes viewpoints held by human groups regarding common ideas and values and plays a role in establishing a shared perspective of acceptable behavior (Dorantes et al., 2006; Ferguson, 1979; Robertson & Fadil, 1999; Simga-Mugan, Daly, Onkal, & Kavut, 2005; Whetstone, 2001). An individual's personal variables such as age, education, emotions, gender, life experiences, and values all contribute to the development of their ethical stance and help guide and delineate "right" conduct (Dorantes et al., 2006; Keller et al., 2007; Simga-Mugan et al., 2005; Trevino, 1986; Trevino et al., 2000). Social interactions such as memberships in social clubs, groups, fraternities, sororities, and other organizations instill a strong sense of belonging as well as expected ethical attitudes and behaviors in society. These influences are powerful, making certain thoughts and actions extremely likely by the individual being influenced (Ambrose, Arnaud, & Schminke, 2008; Ferguson, 1979; Robertson & Fadil, 1999). Personal relationships within families also contribute heavily to the formation of an individual’s ethical foundation. Close friends, peers, idols, and persons emulated or held in high esteem further shape ethical perspectives and impact the development of a person’s sense of right and wrong actions and behavior (Ambrose et al., 2008; Leonard et al., 2004; McDevitt, Giapponi, & Tromley, 2007; Schminke, Ambrose, & Neubaum, 2005).

These external influences pre-exist in an individual prior to employment but are also an ongoing, evolving factor. They affect a person’s values, honesty, reliability, loyalty, integrity, and sense of fairness (Trevino et al., 2000; Whetstone, 2003) and help form an individual’s ethical belief system or moral philosophy which in turn affects their ethical decisions (Singhapakdi, Kraft, Vitell, & Rallapalli, 1996). They also influence how a moral agent interprets and internalizes other external influences. Being cognizant of a person’s core beliefs is essential before behavior change can be affected as part of workforce development, particularly in addressing insider threats (Alfawaz et al., 2010; Boss et al., 2009; Colwill, 2009).

The four TWEB constructs with their virtue ethics based tenets interact with external influences on a moral agent to affect ISS; however, they also may have an effect on how any organizational internal influences such as ethical codes of conduct, polices or training which are implemented by an organization are perceived, interpreted, and acted upon by a moral agent. Researchers have noted that all ethical influences on a moral agent in the context of life and work must be considered (Floridi, 2006) and that external influences such as family and the personal life of employees will affect their behavior at work (McDevitt et al., 2007). Trevino et al. (2000) and Whetstone (2001) concur that what people do in their personal lives carries into the organization that they work for and that it impacts how those individuals interpret and react to organizational influences. The resulting effect of both internal and external influences on the ethicality of people, particularly that of IS trusted insiders is that despite any ethics codes, policies, procedures, or work practices implemented by an organization, the moral agent's own internal sense of ethics and morality will be the primary factors in any ethical decisions they make and will in turn affect the overall IS security posture. By recognizing these internal motivations an organization can use virtue ethics to shape the moral agent's evaluations, actions, and behavior.

When implementing an ethics based model an organization must define what is considered ethical behavior in order to have a frame of reference for desired outcomes. Expected employee behavior should be based on the core principles of the particular ethical philosophy chosen (Weber 1993). The virtue ethics approach focuses on the character of the moral agent involved instead of a specific action and emphasizes that the virtues which make up an individual's character will guide and determine their ethical behavior. The Effects category of the TWEB model is the product of the trusted worker ethical evaluations and actions generated from the relationship and interaction between the ISS constructs and information influencers. Observable indicators of ethical behavior in regards to information systems security include rules compliance, enacting best practices, security incident reduction, loyalty, and a commitment to security.

Rules compliance is evidence that employees are complying with organizational security guidelines, policies, and regulations, following mandated rules of correct behavior, and demonstrating an ability to make the "right" choice in ethical situations (Alfawaz et al., 2010; Lim et al., 2009; Myyry et al., 2009). Enacting best practices means that in the absence of specific guidance employees will utilize or respond with appropriate industry or professional processes when presented with information system security issues (Adam & Bull, 2008; Lim et al., 2009). Incident reduction is corroboration that there has been a reduction or elimination in the number of instances of information loss, compromise, disclosure, or theft (Greenberg, 2002; Van Niekerk & von Solms, 2010). Loyalty entails demonstrating honesty and sincerity to the organization, fellow employees, the IS security profession, and possessing an understanding that there is a collective commitment to each other characterized by mutual dependency and shared benefits. Attributes include self-control and reliability by maintaining ethical standards versus being ethically flexible – meaning that an individual practices situational ethics when presented with security issues that conflict with other dictates (Banerjee et al., 1998; Huff, Barnard, & Frey, 2008a; Leonard et al., 2004; Workman & Gathegi, 2007). A commitment to security is manifested by reporting all known security issues or vulnerabilities which may result in threats to the IS, regardless of whether disclosing those issues is beyond the scope of the individuals job performance requirements, that it may be an unpopular stance, or may result in undesirable consequences to individuals or the organization (Alfawaz, 2010; Lim et al., 2009). Trusted worker ethical behavior indicates the resulting effect that the internal and external influences have on the behavior of a moral agent, who in the context of this study is defined as trusted workers with privileged access to information systems. It is important to note that the effect of influencers on the behavior of a moral agent can be positive or negative.

The TWEB model captures the conclusions that character traits predispose how a person will respond in ethical situations and that an organization can exert influence on employee ethical behavior (Huff et al., 2008a; Kaptein, 2008; Trevino, 1986, 1990). It is intended that the model will be used to guide the research effort by illustrating relationships between the individual variables.

3.4 Research Hypotheses

Founded in the review of relevant literature and utilizing the four cardinal virtues as defined by Aristotle (2005) and Aquinas (2005) as a basis, the objective of this study was to confirm through statistical validity the four virtue ethics based constructs as they relate to information system security. The focus was on validating construct indicators and factors that influence the ethical commitment of information system workers in trusted positions through examination of the components and their relationships in the TWEB model. Four formative constructs form the basis of the model. A formative construct, also known as a composite latent variable, assumes that measures or indicators cause the construct therefore the direction of the causality is from the indicator to the construct (Jarvis, MacKenzie, & Podsakoff, 2003). The indicators may or may not be correlated to each other or have an effect on each other. The indicators were considered formative or casual as changes in them determine the characteristics of the associated construct. The

TWEB model was used as a basis for conducting empirical testing of the constructs for validity.

It was found by Myyry et al. (2009) that the influences on the components of ethical decision making processes regarding ISS policy compliance merited further research. Whetstone (2005) notes that virtues are essential attributes and that they must be assessed and adjusted according to their context. This research study endeavored to assess and validate ISS constructs as part of a trusted worker ethical behavior model based on the cardinal virtues without any loss of meaning, and suggest how they influence the moral choices of information system security workers. These influencers fit into the info-influencer component of the revised information ethics model as depicted in Figure 4.

Based on the literature review and the goals of this study, which were to determine the applicability of the cardinal virtues and to identify key elements of virtue ethics which may be applicable to ISS in order to better understand those individuals who may be an insider threat to an information system, the following statistical hypotheses were tested:

H1: Increased ISS Astuteness will have a positive effect on trusted worker ethical behavior.

H2: Increased ISS Conviction will have a positive effect on trusted worker ethical behavior.

H3: Increased ISS Rectitude will have a positive effect on trusted worker ethical behavior.

H4: Increased ISS Self-Discipline will have a positive effect on trusted worker ethical behavior.

H5: Organizational internal influences moderate the effect of the four virtue ethics constructs on trusted worker ethical behavior.

H6: External influences on trusted workers moderate the effect of the four virtue ethics constructs on trusted workers.

H7: External influences on trusted workers affect how organizational internal influences are interpreted.

A path diagram corresponding to the casual relations among the variables in the TWEB theoretical model is shown in Figure 6, TWEB Model Hypothesized Relationships.

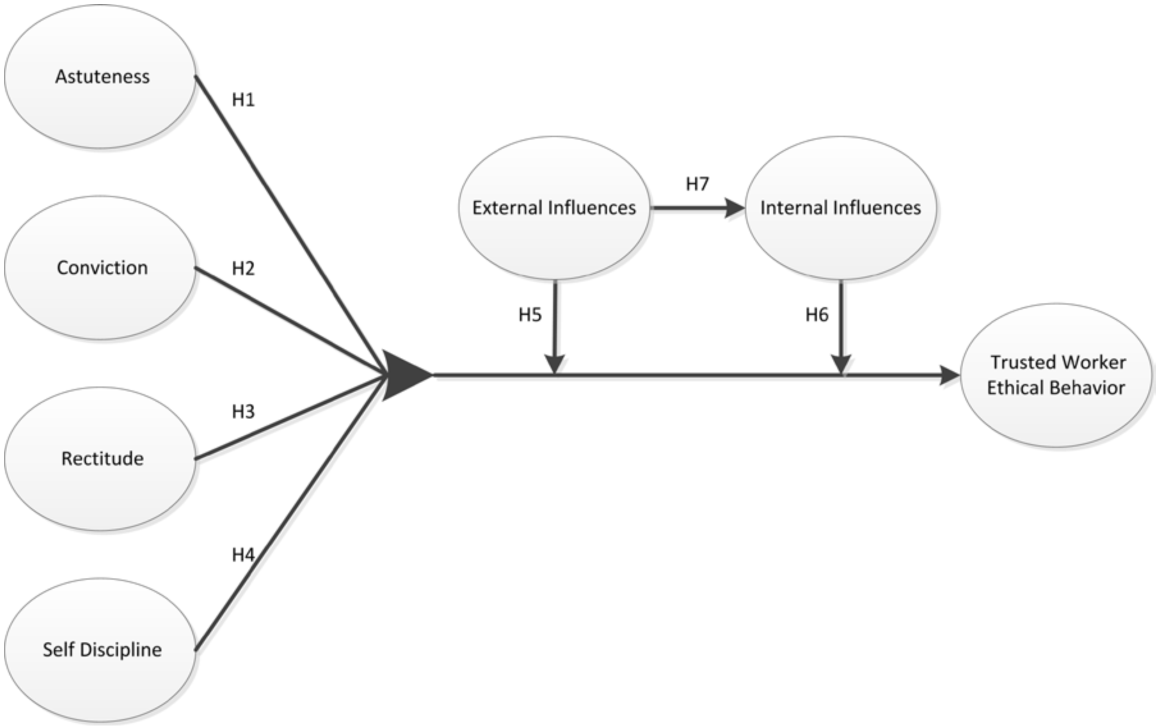


Figure 6: TWEB Model Hypothesized Relationships

To test the hypotheses, the validity and reliability of the proposed ISS constructs, associated indicators, and the proposed theoretical model was verified by conducting and interpreting Confirmatory Factor Analysis and Structural Equation Modeling. Results of the statistical analysis provide empirical evidence to aid in determining if a virtue ethics based approach to affect a moral agent's ethical decision making is valid in an ISS setting.

3.5 Research Method

According to Leedy and Ormrod (2005) the primary purpose of the research methodology is to dictate and control the collection of data and to organize and interpret meaning from it. In social sciences fields such a management information systems the use of the survey methodology is one of the dominate methods to gather data in IS research (King & He, 2005) and is a common way to empirically study the characteristics and relationships of variables (Roberts, 1999). The non-experimental, descriptive research method utilized for this study was an electronic survey to facilitate the collection, analysis, and integration of research data regarding the proposed measures for virtue ethics based constructs that may influence the ethical choices of ISS trusted workers. This methodology allowed for anonymity of the participants. The survey instrument was based on quantitative research which allows for investigation of phenomena through statistical techniques because the data is in numerical form (Sekaran & Bougie, 2010). This is important because it provided a means of making a mathematical connection between the observed data and the proposed relationships. The quantitative data collected was used to analyze the constructs and theoretical model using Confirmatory Factor Analysis (CFA) and Structural Equation Modeling (SEM). Quantitative data is considered more efficient and reliable by many researchers and is often used to test hypotheses; however, one criticism is that it misses contextual detail (Creswell, 2003). Survey research uses questions to represent measured variables and relies significantly on factor and path analysis processes. The participants were members of a national information system security organization. The professional background of the membership included information systems (IS) executives, information technology specialists, and university students enrolled in an IS or ISS program.

A non-experimental or non-manipulative research method describes behavior such as what people do or think without identifying the cause or reason for the behavior while also providing valid statistical data. Consistent with the non-experimental research methodology, for this study an anonymous survey delivered via an Internet website was used as it was determined that it would be less threatening to responders and potentially increase the response rate and validity of answers. Research by Stritzke, Nguyen, and Durkin (2009) demonstrates that anonymous computer mediated communications are less threatening and result in a higher rate of participation. Surveys are suitable for capturing data about issues and problems where there is incomplete information; however, respondents must be confident that the survey is anonymous in order to elicit honest answers. Additionally, research biases such as those introduced by face to face or telephone interviews are minimized (Roberts, 1999). The survey research method supports the study of cultural and social problems and events; captures the point of view, feelings, and opinion of participants; and is consistent with the design of previous research studies on ethical behavior, attitudes, and morality (Fowler, 2014; Rea & Parker, 2005). It is a proven way to capture the ethical climate within an organization. Additionally, surveys are an important and accepted method for conducting theory validation and demonstrating external validity in the field of IS (King & He, 2005).

Because there are quantifiable measures of the variables this study on information systems was classified as positivist (Klein & Myers, 1999) and because the data was collected from humans it was subjective. This type of research method is an accepted method used to advance scientific knowledge (Pinsonneault & Kraemer, 1993; Skulmoski, Hartman, & Krahn, 2007).

Factor analysis was used to provide insight into the data obtained in the survey. CFA is typically used to test a theory when prior research shows strong evidence of what factors should be included and what indicators should define them (Henson & Roberts, 2006). Data for conducting CFA and SEM is typically obtained utilizing surveys and is used to demonstrate casual patterns in sets of variables (Stage, Carter, & Nora, 2004). Using this data the constructs were assessed for their validity and reliability in the proposed ISS Trusted Worker Ethical Behavior model through CFA to test whether they were consistent with this researcher's understanding, then tested for casual relations through SEM. Use of SEM techniques is accepted in information system research and is on the increase according to Freeze and Raschke (2011).

3.5.1 Instrument Development

Theory testing and development research uses measures or indicators to provide empirical estimates for theoretical constructs. One way a construct obtains meaning is by having observable indicators. Development of measures is necessary prior to validation testing of the associated construct model by CFA and SEM. Jarvis et al. (2003) contend that in the past researchers have made a greater effort in justifying theoretical structural relationships and their direction of causality rather than establishing or detailing their construct measurement relationships, and advocate that each should be justified and tested. They also note that previous research has shown that it is necessary for a measurement model to be properly specified before any meaning can be given to the analysis of the related structural model; however, in the past researchers have generally given little attention to proper direction of causality in measurement relationships. Petter et al. (2007) concur that the relationship between constructs and their measures is often ignored by researchers. Using a scale development process proposed by MacKenzie et al. (2011) the formative constructs and their measures were defined and validated by in order to better understand the components and characteristics of virtue ethics as they apply to ISS (Gray & Tejay, 2014, 2015).

MacKenzie et al. (2011) noted that the concept of a construct is that it is a nebulous concept or variable that is put together in a person’s imagination, it is known to exist but is not directly observable, and that it is more general than specific in nature. They recommend a ten step process, the Scale Development Procedure, for construct and measurement development and validation, illustrated in Figure 7. Scales are observable items that capture pieces of the concept and when combined form the construct. These items are typically represented as statements regarding attitudes or beliefs. Construct validity is defined as the degree of relationship between a construct and its indicators or measures (Jarvis et al., 2003). Construct conceptualization was accomplished through a literature review of previous theoretical and empirical research and in discussions with numerous IA and ISS practitioner subject matter experts (SMEs) in order to identify the

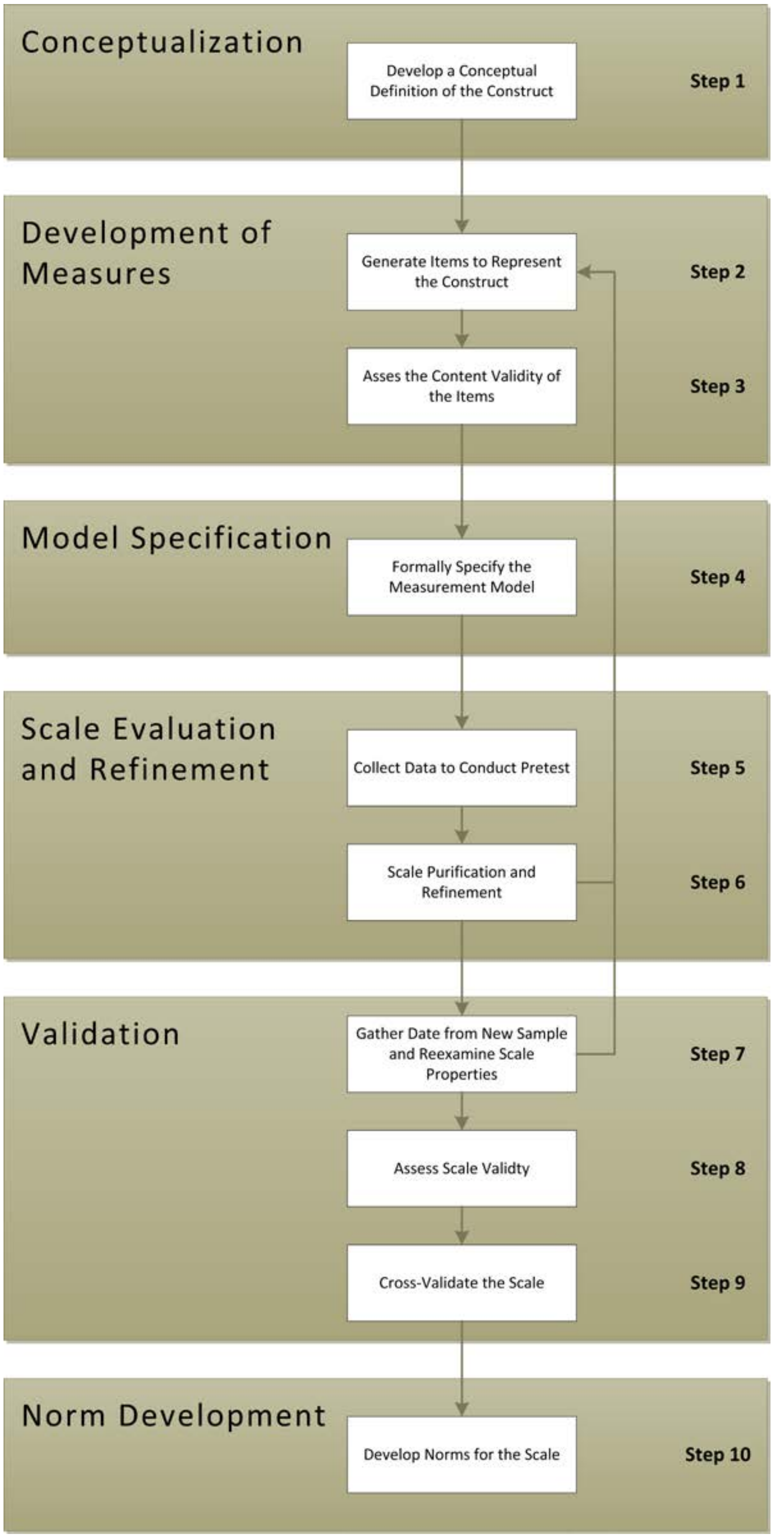

Conceptualization
Develop a Conceptual Definition of the Construct
Step 1
Development of Measures
Generate Items to Represent the Construct
Step 2
Asses the Content Validity of the Items
Step 3
Model Specification
Formally Specify the Measurement Model
Step 4
Scale Evaluation and Refinement
Collect Data to Conduct Pretest
Step 5
Scale Purification and Refinement
Step 6
Validation
Gather Date from New Sample and Reexamine Scale Properties
Step 7
Assess Scale Validty
Step 8
Cross-Validate the Scale
Step 9
Norm Development
Develop Norms for the Scale
Step 10

Figure 7: Scale Development Procedure

From "Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques," by S. B. MacKenzie, P. M. Podsakoff, and N. P. Podsakoff, 2011, MIS Quarterly, 35(2), p.297. Copyright 2011 by MIS Quarterly. Reprinted with permission.

key characteristics of the proposed constructs. Then each construct was placed in a conceptual domain which identified the general property the construct represented and the entity to which it applied to as detailed in Table 4, ISS Construct Conceptual Domains. A conceptual domain is the general property type that the construct refers to or represents (MacKenzie et al., 2011). If the measures conceptually represent the conceptual domain they can be considered adequate for use in empirical predictions (Coltman, Devinney, Midgley, & Venaik, 2008).

Next the conceptual theme, consisting of the fundamental characteristics that were considered necessary for each construct, were determined as identified in Table 5, ISS Construct Conceptual Theme Attributes. Once the conceptual themes for the proposed constructs were identified each was categorized as multidimensional because it was determined that their defining attributes were distinct but related, therefore the four constructs could be collectively conceptualized or treated as one composite theoretical concept or dimension - specifically that of ISS Virtue Ethics, such as the models with multiple formative constructs detailed by Diamantopoulos et al. (2008) and Williams, Edwards, and Vandenberg (2003). The TWEB model constructs are deemed formative because of the relationship of the indicators to them; specifically that the indicators create

Table 4: ISS Construct Conceptual Domains

Construct	General Property Represented	Applicable Entity
ISS Astuteness	Professional Competency	IS Trusted Worker
ISS Conviction	Beliefs and Intentions	IS Trusted Worker
ISS Rectitude	Fairness of Actions	IS Trusted Worker
ISS Self-Discipline	Personal Behavior and Conduct	IS Trusted Worker

and summarize the theoretical construct rather than being reflective aspects of the construct.

Table 5: ISS Construct Conceptual Theme Attributes

Construct	Necessary/Essential Attributes
ISS Astuteness	- acute mental vision - practical know-how - intelligence
ISS Conviction	- certainty of one's beliefs without need for proof - confidence in one's own abilities and decisions - positiveness in one's own mind of something that is right
ISS Rectitude	- right conduct - morally correct behavior - honest, decent character
ISS Self-Discipline	- persisted willpower - self motivation - personal conduct controlled by structured thought

In Development of Measures, Step 2, construct validations of the new measures began with item generation with the primary concern being content validity (Hinkin, 1995). Using prior research, reviews of literature, and opinions of practitioners and SMEs is an accepted method of construct conceptualization and development (MacKenzie et al., 2011). A review of relevant literature identified the generally accepted indicators of the virtue ethics constructs of temperance, fortitude, prudence, and justice and facilitated item generation of potential indicators for each of the proposed formative constructs of ISS Astuteness, Conviction, Rectitude, and Self-Discipline as they relate to IS security as summarized in Table 1. The content validity of the construct indicators were then preliminarily assessed and the measurement scales refined through the use of a Delphi study (Gray & Tejay, 2015). As noted by Avery et al. (2005) and Lummus, Vokurka, and Duclos (2005) the Delphi method is widely used to generate ideas and solutions via group interactions between anonymous experts, specialists, or informed advocates rather than through random population samples. Using the Delphi technique in Step 3 of the Scale Development Procedure capitalized on the professional experience and subject matter understanding of SMEs in order to identify the key measures or indicators of virtue ethics based security constructs by facilitating the aggregation and distillation of opinions through controlled feedback.

The results of the Delphi survey were used to refine the construct measures down to the most applicable, content valid indicators. Typically after measures evaluation, each construct should have a manageable number of indicators, but at least three to four per construct to ensure proper identification (Hall, Snell, & Foust, 1999). Each of the proposed constructs had at minimum five measures to be evaluated. The indicators which were retained after the purification effort by the Delphi panel were further refined and validated in a quantitative study in a directed research study by Gray (2013) who followed the Scale Development Procedure.

It is necessary that a measurement model is properly specified and a determination made that the measurement model is valid before any meaning is given to the analysis of the related structural model (Bollen & Lennox, 1991; Jarvis et al., 2003). Accomplishment of the items in Step 4, Model Specification, set the presumed relationships between the indicators and the represented construct and has resulted in formally specifying the measurement model by generating individual content valid construct indicators. Using individual items helps to ensure that the overall testing of a measurement model is more stringent because more covariances must fit, thereby helping to identify items which are unsuitable for inclusion into the model. The final area addressed by the directed research study (Gray, 2013) was Steps 5 and 6 of the scale development procedure, Scale Purification and Refinement, where data was collected in an electronic survey and the construct indicators were validated and assessed for reliability. Having constructs defined by measures is necessary before a relationship between constructs can be analyzed in a structural equation model (Diamantopoulos, Riefler, & Roth, 2008, 2008; MacKenzie et al., 2011). Based on the research by MacKenzie et al. using the Scale Development Procedure to establish construct indicators was an appropriate solution that was particularly well-suited for producing valid results.

Results of the directed research study provided a collection of validated indicators for each of the four proposed ISS virtue ethics based constructs. Those four constructs comprise the basis of the TWEB theoretical model that were to undergo further testing using confirmatory factor analysis and structural equation modeling techniques. Previous researchers have noted that theoretical models were developed based on constructs of which the indicators were not adequately defined. Therefore, this information is included as background in this research study in order to demonstrate that the four proposed constructs which form the basis of the trusted worker ethical behavior theoretical model are comprised of indicators derived from empirical data.

3.5.2 Phases of Research Study

The focus of this research study was the TWEB model, consisting of seven factors or constructs, and was based on prior research conducted with ISS professionals (Gray & Tejay, 2014, 2015). Researchers use theoretical models to understand underlying processes, therefore the TWEB theoretical model was being proposed and evaluated because previous research has not produced a set of virtue ethics based security constructs applicable to ISS. The research was performed in four phases, illustrated in Figure 8, Research Study Phases.

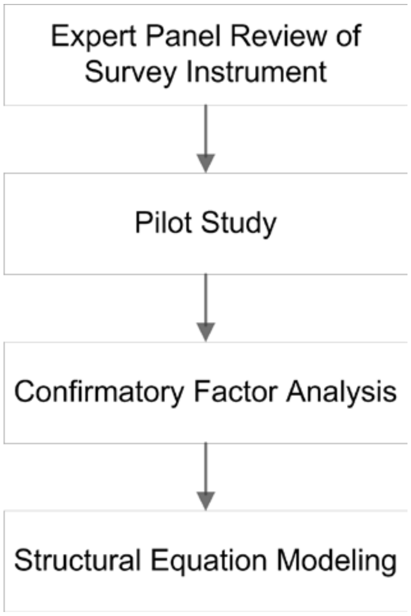

Expert Panel Review of Survey Instrument
Pilot Study
Confirmatory Factor Analysis
Structural Equation Modeling

Figure 8: Research Study Phases

Expert Panel Review

Survey instruments are used to collect data to produce empirical results in research studies. Straub (1989) noted the importance of validating positivist, quantitative management information systems research instruments in order to substantiate that any instruments developed in fact measure what they purport to measure. For this study, after a review of related instruments for potential usability, an original survey instrument was developed and validated using methods specified by Lewis, Templeton, and Byrd (2005), Lynn (1986), and Straub. In the first phase of the research study development and validation of the instrument and its items were facilitated by utilizing a panel of IA and ISS subject matter experts who were knowledgeable in the studies concepts to provide content evaluation, verify content clarity, and identify any ambiguous or confusing statements or any other problems.

Item content validity demonstrates how well each indicator measures the content domain it is supposed to measure. Assessment of content validity is a multi-stage process typically consisting of a literature review or content analysis and item screening through judgment and quantification by a specific number of experts (Lewis et al., 2005; Lynn, 1986; Roberts, 1999, Straub, 1989). Petter et al. (2007) state that in the case of formative constructs content validity is established through literature reviews and determinations of expert panels. The literature review was previously accomplished and the results used to develop a survey instrument. Having SMEs review the content of the survey instrument served to establish content validity and eliminate irrelevant items (Hyrkäs, Appelqvist-Schmidlechner, & Oksa, 2003; Lynn, 1986). Expert status was established by verifying that each panel member holds a CISSP certification. The International Information Systems Security Certification Consortium (ISC²), the accrediting authority for the certification mandates that CISSPs possess a minimum of five years of direct, full time IS security work experience in at least two information security domains. The CISSP certification serves as globally recognized confirmation of an individual’s knowledge and experience in the ISS field and is arguably the most recognized practitioner ISS certification. Using between five and ten experts who achieve 80% agreement on an item as being valid to a construct provides a reliable determination of content validity (Hyrkäs et al., 2003; Lynn, 1986) while Hinkin (1998) states that 75% agreement is acceptable for evidence of content adequacy. Based on Hinkin's tutorial for development of measures used in survey questionnaires a 75% level of agreement among the expert panel was used to retain construct indicators.

A panel of ten SMEs was recruited to conduct the review of the survey instrument, each assessing it for content, clarity, ambiguity, and relevance. The panel was also provided an opportunity to suggest improvements to the wording of the construct indicator statements. Completion of the expert review established the extent that the survey instrument covered the concepts it purported to measure. The review process identified that for the construct of ISS Astuteness the content validity and relevance of four measures did not reach the required level of agreement as the panel felt the content was covered by other indicators. Therefore, the four measures - specifically those of ethical behavior involves intellect, ethical behavior involves responsible use, employee values affect security compliance, and logical decisions affect security were eliminated. All other indicator statements received a 75% or greater level of agreement. The panel also recommended improvements to the wording of eight other indicator statements to improve clarity of meaning. Those recommendations were incorporated.

Proactive measures were taken to prevent common method bias, where spurious variance is attributable to the measurement instrument or method rather than to the constructs the measures are assumed to represent. As recommended by Podsakoff, MacKenzie, Lee, and Podsakoff (2003), survey items were ordered by placing the endogenous construct indicators prior to other items, and the survey itself was anonymous.

Pilot Study

The second phase consisting of a pilot study was conducted to pre-test the survey instrument. Pilot studies are important because they are dress rehearsals for the conduct of the survey; further appraise the content of the instrument; determine if the survey instrument is too long, too complicated, or needs clarification; assess whether the research method is realistic and workable; assess participant recruitment issues; identify difficulties or problems in completing the survey and any ambiguities or other participant concerns or suggestions by soliciting feedback; as well as establishing the approximate survey completion time (Lewis et al., 2005; van Teijlingen & Hundley, 2002).

Pilot study practitioner participants were recruited and the survey administered to these participants in exactly the same manner as it would be to participants in the main study. It also included several administrative and instructional design professionals in order to solicit their feedback on survey instrument presentation and formatting. This contributed to identifying issues with the presentation method and helped to determine the amount of time required to complete the questionnaire. Feedback resulting in improvements to the survey process or instrument was documented as recommended by van Teijlingen and Hundley (2002). Lancaster, Dodd, and Williamson (2004) note that the number of participants in a pilot study is dependent on the statistical parameters the researcher wants to achieve in the main study with a minimum of 30 participants being recommended. The pilot study in this research was not used to set statistical parameters; however, the recommendation for at least 30 pilot study participants was followed. Thirty-eight individuals were recruited of which 31 actually participated. One respondent did not complete the survey, resulting in 30 complete responses which provided feedback.

With the exception of one construct indicator item all suggested changes were related to the survey information and instruction sections. Specific items recommended for improvement included shortening run-on sentences and consistency in capitalizing the terms information systems and information systems security. The construct indicator which was identified as unclear by five participants was survey question F-3, which was modified as recommended for clarity. The majority of the participants found the survey to be easy to take, well organized, and that it had good functionality. Results also indicated that the survey would take between 10 and 15 minutes to complete.

After incorporating the changes suggested by the expert panel review and pilot study pilot study the survey instrument was finalized and ready for use. The wording version used in the survey instrument for the descriptions of the indicators is detailed in Appendix B, Research Model Variables and Indicators.

CFA and SEM

In the next two phases of the research CFA and SEM was used to test specific hypotheses regarding the nature of the model's factors or constructs. The SEM modeling technique is particularly well suited for research in information systems as one its strengths is being able to discover or confirm relationships between observed and latent variables through the analysis of observable indicators or measures (Dow, Wong, Jackson, & Leitch, 2008). The first component of SEM is CFA, a form of factor analysis used in research to test sets of constructs and confirm measurement models. The measurement model is the part of a SEM model which deals with constructs – also termed as latent variables, and their indicators. It relates a particular construct to its associated indicators or measures (Jarvis et al., 2003). SEM is used to analyze the structural or path relationships between constructs – a model's latent variables and observed variables. Statistical techniques such as CFA and SEM are also used to lower the numbers of observed measures or variables by determining the covariation within the observed variables (Schreiber, Nora, Stage, Barlow, & King, 2006). A conceptual structural equation model of TWEB, Figure 9, depicts the measurement and structural components, their relationships, and the construct categorization as either formative or reflective.

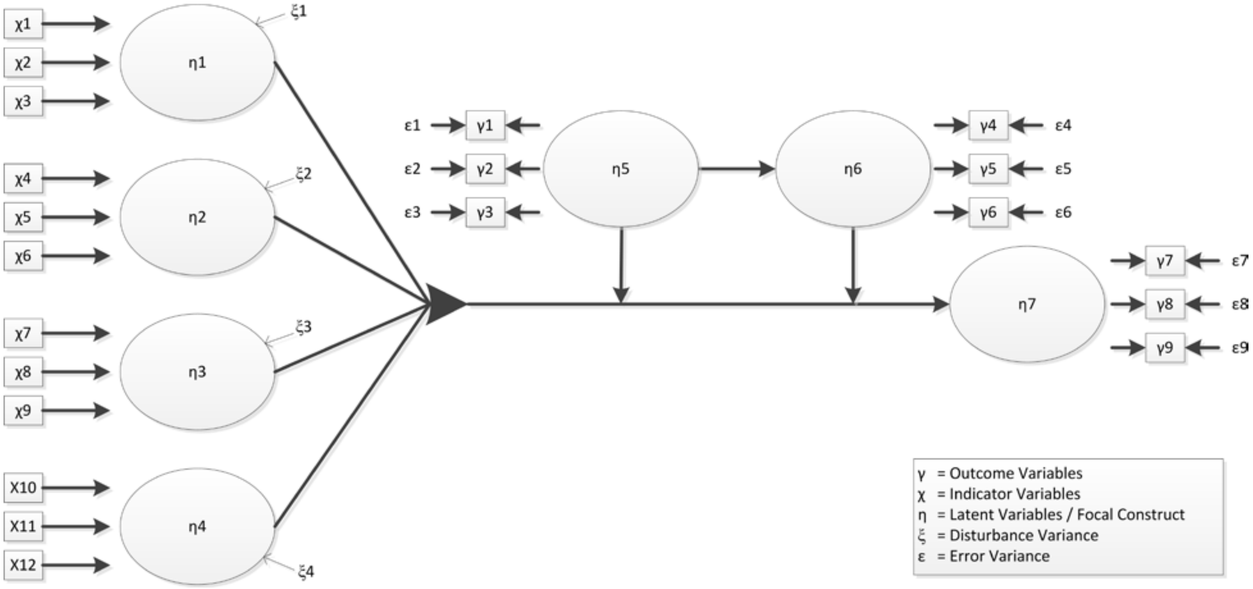


Figure 9: Conceptual SEM of TWEB

In the third phase of the research study CFA was performed on the measurement model to determine if a relationship between the observed variables and their underlying latent constructs existed and whether the observed indicators accurately described the theoretical constructs; with construct validity being the extent that the indicators reflected or captured the concepts they were supposed to be measuring as recommended by Chandler, DeTienne, McKelvie, and Mumford (2011). In this phase research hypotheses' testing is supported by using a research model to provide a visual representation of the constructs, measure or indicator variables, and the proposed interrelationships in order to facilitate assessment of how strongly the variables are related. CFA provided quantitative measurement of the reliability and validity of the models constructs through several tests to assess which measures or indicators fit each factor, determine if the factors were correlated or uncorrelated, and identify the correlations between variables. The survey data collected was used to test how well the measured variables – each construct's indicators, represented their associated construct using the appropriate indices as identified in the Data Analysis section.

Finally, in the last phase SEM was used to perform path analysis on the structural model to estimate how well the hypothesized model fit the observed data set. Path analysis is used in research to examine and test models, particularly those which have chains of influence between numerous variables (Streiner, 2005). The TWEB structural model was tested using the indices identified in the Data Analysis section.

Using the CFA and SEM research methodology provided the means to test the validity of the construct indicators, relationships between construct (factor) loadings, determine whether they are correlated or uncorrelated, and evaluate the fit of the hypothesized model to the observed data set thereby providing a basis to confirm or reject the study's hypotheses. The details of the measurement model and structural model data analysis are presented in Chapter 4.

3.5.3 Data Collection

Data collection was facilitated through an Internet based survey service, SurveyMonkey (www.surveymonkey.com), who delivered the online questionnaire and compiled the resulting data. There are two primary issues to be concerned with when performing data collection; ensuring that the sample being surveyed represents the population they represent, and the size of the sample (MacKenzie et al., 2011; Sekaran & Bougie, 2010). The sample must be representative of the population in order for the survey to have meaning. The demographics information collected in the survey were used to support that the sample was representative of the ISS professional population.

Regarding sample size, large samples improve statistical power (Roberts, 1999). However, if the indicators demonstrate communality, termed as the extent which an indicator correlates with the other indicators, and are comprised of strong, clearly defined indicators then the sampling error will be small, therefore smaller survey response numbers, in the order of 60-100, are sufficient for validity. Otherwise higher sample numbers are necessary for validation (MacCallum, Widaman, Zhang, & Hong, 1999). Ensuring that these two sample size requirements are met enables the evaluation of the scale to determine the degree a construct behaves as it should within a system of related constructs; specifically that the measures of constructs which theoretically should be related are in fact related, and if measures that should be unrelated are in fact unrelated (MacKenzie et al., 2011).

Research by Gagne and Hancock (2006) contends that calculating sample sizes is challenging but required so as to provide a basis for the quality of the measurement model and to increase construct reliability in CFA and SEM. It is also noted by Lenth (2001) that determining the appropriate sample size of a study is difficult; it must be large enough to be statistically significant in order to provide useful results, yet not so large as to waste the researcher's resources. Lenth also points out that the primary goal of the researcher should be to design a high quality study, and makes recommendations that help establish sample sizes and power. The approach this study took to determining sample size was based on the recommendation of specifying the confidence interval, confidence level, and population size.

A confidence interval is the margin of error that can be tolerated in the results. Assuming that respondents are split 50-50 in their survey answers then a lower margin of error will require a larger sample size. The confidence level is the amount of uncertainty that can be tolerated in the results. A 95% confidence level means that there would be a 95% chance that the survey result in question would be within the margin of error. The size of a population is also a determinant, and statisticians generally agree that sample size requirements do not increase much for populations of more than 20,000; consequently this was an assumption of this study. The membership of the professional organization which participated in this research study's survey exceeds 20,000 so this number was used for the population size. A sample size calculator freely available from MaCorr Research Solutions was used to identify a range of samples sizes. Table 6, Study

Sample Size Determination, presents the minimum recommended sizes based on a various confidence levels and intervals.

It was this researcher's goal to achieve a minimum usable sample size of 377 respondents in order to achieve a confidence level of 95% with a confidence interval of 5%. A total of 441 individuals participated in the survey. Of those that responded 46 did not complete the entire questionnaire therefore those responses were discounted, yielding 395 surveys that were usable for data analysis. The statistical strength of this study's results based on the number of usable responses and the determinations in Table 6 is a confidence level of 95% with a confidence interval of 5% (actual was 4.42%).

In the test-retest survey used to establish indicator reliability over time a total of 157 individuals indicated they would participate, and 97 actually responded. Of those that responded 6 did not complete the entire questionnaire therefore those responses were discounted, yielding 91 surveys that were usable for data analysis. The statistical strength of this study's results based on the number of usable responses and the determinations is a confidence level of 95% with a confidence interval of 6.68%.

A critical component of survey based research is the selection of appropriate survey participants as it is their expert opinions that form the basis of the survey output. The unit of analysis - the major entity being analyzed in this study, were individual IS professionals in the IS/ISS field. Consequently, this study's survey was delivered to selected individuals who were members of a professional community of information assurance (IA) and cyber security professionals. The answers those individuals provided to the survey questions comprised the data which was statistically analyzed. In order to gather a representative sample from across the entire spectrum of the profession, data was

Table 6: Study Sample Size Determination

Confidence Level	Confidence Interval (margin of error)	Sample Size
95%	5%	377
95%	7.5%	169
95%	10%	96
95%	12.5%	61
90%	5%	269
90%	7.5%	120
90%	10%	68
90%	12.5%	43

solicited from personnel employed in IT positions such as IS executives, managers, professionals, and university students enrolled in IA, IS, or ISS focused programs. As recommended by Goodman (1987) potential survey participants were not be randomly targeted, but identified as being either experts or informed advocates. Participant eligibility and selection criteria included one or more of the following characteristics:

- employed in the IT profession
- enrolled in IA/IT/IS/ISS university classes
- position title that reflects direct involvement with ISS in an oversight capacity
- member of an ISS organization

Consent to conduct the study was obtained from Nova Southeastern University via the Institutional Review Board (IRB) process, Appendix D, and the participating professional organization prior to distributing the survey questionnaire. The survey was distributed via email to potential participants with an invitation to participate via an Internet link and it was open for participation for approximately twelve weeks. During the time the survey was open the individual chapters of the organization being surveyed distributed the survey link to their members. Additionally, the snowballing technique where survey participants are invited to recommend to colleagues they deem qualified to take part in the survey was allowed. Response numbers were monitored throughout the survey process; after 400 responses were received the results were reviewed for completeness to ensure that the required number of completed surveys needed to achieve the desired confidence level and confidence interval were obtained. Once these numbers were achieved the primary survey was closed. Numerous participants volunteered an email address in which to facilitate participation in a test-retest survey. Participants were provided assurance that only the researcher would be able to associate their individual responses to that email address and that this information would remain confidential. The follow-up test-retest survey which was used to establish indicator reliability over time was closed 25 days after the last reminder was sent to participants.

The initial web page of the survey included a consent for participation condition; if participants did not accept the conditions they were not allowed to proceed with the survey. The survey took participants approximately 15 minutes to complete and because it was anonymous it had to be completed in one session. The extent of researcher influence on the study participants was deemed minimal, limited to analyzing and interpreting data collected via the online survey. The identity of the researcher was known to the participants; however, participants were assured that their individual responses to survey questions would remain confidential and that their identity would not be revealed even after the completion of the final report. The objective of the survey was to gather data to be used to statistically validate the virtue ethics based security constructs through confirmatory factory analysis (CFA) and test the validity of the ISS Trusted Worker Ethical Behavior Model through structural equation modeling (SEM).

The survey consisted of 44 questions divided into two sections. Section One was used to gather the demographic data of the participants in order to establish the credibility and validity of their IS or ISS background. This was important because if the panelists were shown to have knowledge of the topic under study then validity of their responses could be assumed (Goodman, 1987). Section Two of the survey consisted of indicator statements that focused on potential behaviors, behavioral influences, and their implications on ISS workers. The 38 items in Section Two were rated on a five point Likert-type scale with answers ranging from Strongly Agree to Strongly Disagree, reflecting the extent of the respondents' feelings or strength of agreement in regards to the question. These Likert-type scale closed question responses were used as the basis for developing the statistical comparisons and correlations between variables.

The Likert scale is the most frequently used method to measure attitudes and behaviors in organizational research (Sekeran & Bougie, 2010). Likert scale items provide examples of observed measures or indicators that represent unobserved variables (Schreiber et al., 2006). Research by Weijters, Cabooter, and Schillewaert (2010) found that participants completing surveys with 7-point scales are more susceptible to picking one or other of the endpoints, known as extreme responding. They also found that participants are also more likely to make mistakes when just the end-points were labeled and recommended use of 5-point scales with each item on the scale fully labelled. However, a study by Finstad (2010) advances that 5-point Likert-type scales are more likely than 7-point scales to elicit responses outside the bounds presented to the survey taker. This is termed as interpolation, and is interpreted as evidence that 5-point Likert scales may not be sensitive enough to record a participant's true evaluation of a system. Likert scales with 7 points generate data with higher precision according to Munshi (2014). Sauro (2014) concludes that for single item questionnaires a 7 or more point scale should be used, but for multiple item questionnaires the benefits will be less apparent, and stresses the usability effect of fewer choices. As the web survey format utilized in this research study did not allow for interpolation and the benefits of a 7 point scale seemed to be otherwise minimal to the researcher, a 5 point Likert-type scale was utilized with the intent of lessening the possibility of survey fatigue by the participants.

Despite the findings of Swain, Weathers, and Niedrich (2008) that reversed Likert items have a higher incorrect response rate, questionnaire design for multi-item Likert-type scales commonly include non-reversed and reversed items with the intent of reducing participant inattention, acquiescence bias, and straight line responses (Schmitt & Stults, 1985). To address this issue Weijters et al. (2010) recommend that the reversed items be dispersed throughout the survey, with buffer items separating them. In this study's survey, presented in Appendix C, approximately one-third of the indicators being assessed were written as reverse coded items and they were interspersed randomly throughout the survey questionnaire. In Appendix C, the Survey Instrument , Section Two these are identified by an (R) after the statement in order to make them easier to identify during data analysis. The survey actually presented to the participants did not include this identifier. One free form text box question solicited feedback, comments or recommendations from respondents regarding the survey.

3.5.4 Data Analysis

There are two approaches to conducting SEM, covariance and component based. Formative constructs must have a disturbance or residual term associated with them in order to support the use of the covariance based method. The lack of an error term leads to the problem of the formative construct not being able to be uniquely defined or identified (Petter, et al., 2007; Treiblmaier, Bentler, & Mair, 2011). Solutions to this identification problem include having formative constructs identified through two paths of either measurement relations, structural relations, or a mixture of both; however these solutions must be incorporated into the model prior to collecting data (Petter, et al., 2007). An alternative solution is to utilize component based partial least squares (PLS) SEM as it does not have the constrains caused by formative construct identification issues as all constructs are modeled without error; and its use also has the benefit of removing the possibility of the design of the research model potentially affecting theory development (Cenfetelli & Bassellier; 2009; Hair, et al., 2012). In addition to its use with formative constructs, PLS-SEM is generally thought of as useful only in exploratory research or in studies with small samples; however, Chin (2010) argues that it is complementary to covariance based SEM and may be better suited in some research regardless of construct type, research phase, or sample size. Chin also notes that large sample sizes serve to increase the accuracy of PLS-SEM results; and that it is particularly well suited for research models with complex interrelationships and large numbers of variables. Hair et al. (2011) state that PLS-SEM is more appropriate for theory development research than covariance based SEM.

A covariance-based SEM (CB-SEM) analysis on the formative constructs of the TWEB model following the Treiblmaier et al. (2011) approach for identification was attempted, but was unsuccessful due to it not having incorporated one of the accepted solutions to the identification issue. A second attempt to address the construct identification issue using principal component analysis with split replicated weights as the weighting procedure in order to achieve correlation was also attempted as recommended by Treiblmaier et al. but was unsuccessful. Results were that the covariance matrix was not positively defined and the model did not converge. This result indicated that without modifying the model and collecting new data, component based SEM using PLS was required to address the identification issue. Using PLS was consistent with prior research and analysis of similar models. CB-SEM was used on the reflective constructs of the measurement model.

The collected data was exported to “R”, an integrated suite of software packages which provides a range of statistical analysis capabilities. It is widely used in social science research and has the capability of performing calculations for descriptive statistics including standard deviations, confidence intervals, means, factor loading, and other goodness of fit measures to evaluate models. The R statistical analysis packages Iavaan and PLSPM were utilized as they estimate a variety of multivariate statistical models, including path analysis, confirmatory factor analysis, and structural equation modeling. Gefen and Straub (2005) note that results of a statistical analysis can also be used to perform data reduction, purifying the number of measurement items by dropping any that do not load well. Individual survey responses were consolidated into an average response rating. The size of the survey sample was large enough to provide precision and confidence in the validity of the consensus regarding the applicability of the proposed elements of new information system security constructs. The goal of this study was to conduct statistical analysis at a 5% (0.05) level of significance and this was achieved.

Evaluation of Measurement Model

Development and defining the individual measures and constructs of the theoretical model was previously accomplished as described in chapter 3.3. When establishing the number of construct indicators Dow et al. (2008) caution that models with fewer indicators will have a higher apparent model fit. It is generally accepted that there should be a minimum of four constructs with at least three measurement items per construct (DeCoster, 1998); the TWEB model meets this condition.

One of the purposes for performing confirmatory factor analysis is to analyze the measurement or outer model data in order to establish construct validity (Sun, 2005). CFA evaluation of the measurement model indicates how well the observed indicators load onto and measure their associated construct; and describe their validity and reliability properties to determine whether there is empirical support for the proposed theoretical structure (Schumacker & Lomax, 1996). In order for SEM to be effective in analyzing the model it is necessary to have good data fit (Dow et al., 2008). Observable measures of both formative and reflective constructs are indications of a structural relationship between those indications and a theoretical concept such as the TWEB model (Freeze & Raschke, 2011). In this study the measurement model was identified as having first order formative and second order reflective constructs. Previous information systems researchers have conducted CFA on theoretical models consisting of both formative and reflective measures (Warkentin, Johnston, & Shropshire, 2011); therefore this evaluation approach has a basis in prior research. The TWEB model components of Astuteness, Conviction, Rectitude, and Self-Determination were analyzed as formative constructs; and External Influences, Internal Influences, and Trusted Worker Ethical Behavior were analyzed as reflective constructs. MacKenzie et al. (2011) caution that research in the area of formative constructs measurement is limited and that a consensus among researchers as to the appropriate methods has not been reached. In prior research studies, if identified at all most constructs in measurement models are typically identified as reflective (Jarvis et al., 2003; Petter et al., 2007). However, as noted by Jarvis et al. (2003) the consequences of construct misidentification are that a model may appear to fit the data when in fact it has substantial biases. Evaluation of the measurement model was performed to determine the overall fit of the data by using various researcher community accepted tests for model fit, convergent and discriminate validity, normality, and reliability.

One traditional goodness of fit test is the chi-square measure which is used for evaluating model fit and is a basis for model acceptance or rejection (Hooper et al., 2008). Root mean square error of approximation (RMSEA) is used for measurement and structural fit analysis to account for model complexity and population covariance and is considered one of the most informative model fit indices (Hooper et al., 2008; Kline, 2005). In regards to indices used in CFA, Sun (2005) recommends using Root Mean Square Error of Approximation (RMSEA) for convergent validity and Standardized Root Mean Square Residual (SRMR) for discriminate validity for assessing measurement model goodness of fit assessment; while Jackson et al. (2009) report that relative chi-square (X^2/df) is increasingly being reported as a fit measure. Mackenzie et al. (2011) call for RMSEA and SRMR to be used to assess both formative and reflective construct goodness of fit. Comparative Fit Index (CFI) and Non-Normed Fit Index (NNFI) are fit indices recommended by McDonald and Ho (2002). Boomsa (2000) recommends CFI and if the sample is large NNFI. Finally, GFI, root mean square residual (RMR), NFI, and other goodness of fit tests are identified by Hooper et al. (2008) as well as Schumacker and Lomax (1996) to help measure model validity although they point out that it is not necessary or realistic to utilize every one.

For reflective constructs convergent and discriminate validity are typically evaluated using average variance extracted (AVE) according to Fornell and Larcker (1981) and Hair, Sarstedt, Ringle, and Mena (2012); while MacKenzie et al. (2011) and Straub, Boudreau, and Gefen (2004) recommend assessment of factor-indicator loading. Hair, Black, Babin, and Anderson (2009) recommend assessing item to total squared correlation and item cross-loading as validity checks. For formative constructs Cenfetelli and Bassellier (2009) recommend assessing by indicator loading and weight. Hair et al. (2009; 2012) recommend assessing by indicator weight, cross-loading, path weights and bootstrap confidence intervals. Additionally, Cenfetelli and Bassellier, Diamantopoulos (2011), Hair et al. (2012), and Jarvis et al. (2003) recommend testing formative constructs for multicollinearity.

Kurtosis and skewness tests are commonly used to determine data normality (Kim, 2013; Kline, 1998). Cronbach’s alpha is a coefficient of internal consistency and is a popular statistical procedure used for reliability testing in research involving CFA (Kline, 1998; Tavakol & Denniick, 2011). It is used to measure the reliability of reflective construct indicators. To establish the reliability of formative construct indicators Mackenzie, Podsakoff, and Jarvis (2005) report that test-retest and inter-rater agreement are effective. For hypothesis testing Salkind (2009) describes coefficient correlation and *p*-value as effective methods.

The use of certain fit indices have been criticized and deemed as problematic including GFI because it is affected by sample size (Sharma, Mukherjee, Kumar, & Dillon, 2005), NFI as it is affected by complex models and sample size (Hooper et al., 2008), and chi-square (X^2) because when using large samples it typically rejects almost all models (Hooper et al., 2008). Barrett (2007) does not believe that use of fit indices adds anything to CFA because they allow researchers to claim that mis-specified models are in fact not bad because based on a model's data, a researcher can typically choose whichever fit index that provides the best fit; and therefore recommends that only the chi square index should be interpreted. That recommendation has received considerable criticism and most researchers continue to recommend including the results of some type of fit indices when interpreting CFA and SEM results (Bentler, 2007; Hayduk, Cummings, Boadu, Pazderka-Robinson, & Boulianne, 2007). Jackson, Gillaspy Jr, and Purc-Stephenson (2009) point out that when reporting CFA results there are no set indices recommended for use as fit measures by researchers, however, that cutoff values should be indicated for the measures chosen.

Based on the reviewed research this study utilized the indices of relative chi-square (X^2/df), RMSEA, SRMR, CFI, and NNFI to assess measurement model goodness of fit; AVE, path weights, bootstrap confidence intervals, item to total and squared correlation to assess convergent and discriminate validity; kurtosis and skew for normality; indicator weight and cross-loading for construct indicator validity; Cronbach’s alpha, inter-rater agreement, and test-retest for indicator reliability; coefficient of correlation and *p*-value for hypothesis testing, and multicollinearity to determine correlations between formative indicators. An overview of each of the indices selected for use in the evaluation of the measurement model follows.

Relative Chi-square

Relative chi-square, also termed as normed chi-square, is the value resulting from the chi-square (X^2) index divided by the degrees of freedom and is expressed as X^2/df. It is used to check for over identified models and models that do not fit the observable data (Schumacker & Lomax, 1996). The advantage of this index is that it is less sensitive to large sample size than chi-square alone. Many researchers disregard chi-square (X^2) if the sample size is greater than 200 because it may lead to rejection of an over identified model even though differences between observed and predicted covariances are in fact small. Researcher criterion for acceptance varies, ranging from 1.0 to 5.0 (Schumacker & Lomax, 1996) and 2.0 to 5.0 (Hooper, Coughlan, & Mullen, 2008).

RMSEA

RMSEA is used to assess the absolute fit of a measurement model. It is population based, estimating the amount of error of approximation in each model degree of freedom, taking sample size into account. It is a parsimony adjusted index in that it includes a built-in correction for model complexity, works well with models containing numerous parameters, measures how well tested models represent reality, and assesses how well a model fits in the population (Schermelleh-Engel, Moosbrugger, & Müller, 2003). RMSEA is usually reported with a confidence interval, and acknowledges that it is subject to sampling error (Schreiber et al., 2006). It is considered a “badness of fit” index, meaning that a value of 0 indicates the best fit and higher values indicate a worse fit (Hooper et al., 2008). Values equal to or below 0.05 indicate a close fit, values between .05 and .08 suggest reasonable fit, values of 1 or higher a poor fit (Dow et al., 2008; Hooper et al., 2008; MacKenzie et al., 2011; Schreiber et al., 2006; Schumacker & Lomax, 1996). According to MacKenzie, Podsakoff, and Jarvis (2005) lower RMSEA scores are one of the best indicators of a properly specified measurement model.

SRMR

SRMR is also is used to assess the absolute fit of a measurement model. It is a measure of the mean absolute correlation residual, the overall difference between the observed and predicted correlations. It is an extension of the Root Mean Square Residual (RMR), the square root of the discrepancy between the sample covariance matrix and the model covariance matrix. The RMR range is based on the scales of the indicators in the model which can present problems when a survey instrument contains multiple indicators with varying measurement scales. Because RMR fails to account for the different scales it is difficult to determine whether a given value indicates a good or bad fit (Schermelleh-Engel et al., 2003). SRMR corrects for this by providing a standardized residual matrix which represents the average value across the standardized residual of the data set (Hooper et al., 2008). Values range from 0 to 1, with 0.08 generally considered acceptable and 0.05 or less being well fitting (Hooper et al., 2008; MacKenzie et al., 2011; Schreiber et al., 2006). While the scales used in this study do not vary the SRMR test were performed as recommended by Hooper et al. (2008).

CFI

CFI is one of the most widely used indices in SEM. It compares the sample covariance matrix of the structural target model being tested with that of an alternative null/independence model in which the variables are assumed to be uncorrelated or unrelated (Kline, 1998). CFI represents the ratio between the discrepancies of the target model to those of the null model, and represents the extent to which the target model is better than that of the null model. The statistical range is from 0 to 1, with values closer to 1 indicating a more acceptable fit. Schreiber et al. (2006) identify 0.95 as acceptable. Hooper et al. (2008) recommends 0.90 as acceptable, 0.95 or greater being currently recognized as a good fit, and note that because it is least affected by sample size CFI is one of the most reported fit indices.

NNFI

NNFI, also known as the Tucker Lewis Index (TLI), is an incremental measure of goodness of fit that compares a target model to a baseline or null model. It takes into account the average size of the correlations in the data and the number of parameters in the model; and is affected less by sample size. If the average correlation between variables is low, then the TLI value will be low. This index provides an adjustment to the NFI by incorporating the degrees of freedom in the model to correct for the sensitivity to small sample sizes of the normed fit index, but NNFI itself is sensitive to target model complexity (Hooper et al., 2008; Schumacker & Lomax, 1996). According to Hooper et al. (2008) the values for NNFI should range between 0 and 1, with 0.95 or greater indicating a good model fit. It is noted that because NNFI is non-normed then values can exceed 1, but when that occurs they are adjusted to 1 as that score is considered a perfect fit. Schreiber et al. (2006) suggest a level of 0.95 or greater for acceptance while Schumacker and Lomax state that 0.90 and greater are a good fit.

AVE, Indicator Weight, and Loading

Construct validity or measurement validity is defined as whether the measures or indicators that have been chosen capture the essence of the construct they claim to measure. Three different but interrelated components of construct validity are; convergent validity, discriminant validity, and reliability (Gefen & Straub, 2005; Peter, 1981). Convergent validity proves that two measures of a specific construct that theoretically should be related are in fact related and that the measurement or indicator variables correctly measure the proposed construct or unobserved variable. If the indicators or variables do not correlate well with each other within their parent construct, meaning that the construct is not well explained by its observed variables, then the construct is considered to have convergent validity issues (Fornell & Larcker, 1981; Hair et al., 2009; Peter, 1981). AVE is used as measure of convergent validity, and can be demonstrated by indicators having high loadings on a construct (Gefen & Straub, 2005; Kline, 1998) with values above 0.6 and above loading highly, above 0.4 being significant, and 0.5 or greater being considered an acceptable threshold (Gefen & Straub, 2005; Hair, et al., 2009). An item to total correlation can also be used to determine if an item should be included in the set being averaged. A value of less than 0.2 or 0.3 indicates that the item does not correlate very well with the construct items overall (Nunnally & Bernstein, 1994). Freeze and Raschke (2007) and MacKenzie et al. (2011) state that for formative constructs validity is based on the strength of the path of an indicator to its construct and that convergent validity is not applicable. While Jarvis et al. (2003) also note that formative constructs and their indicators may or may not be correlated; they suggest that researchers should also check for nomological validity, implying there may be some value in conducting a convergent validity test. Bollen and Lennox (1991) agree that in the case of formative constructs the degree of correlation between indicators is not restricted. To support the contention that the TWEB measurement model is comprised of formative constructs convergent validity checks were performed. Nomological validity, also known as law-like validity, evaluates the validity of a construct by examining if its measure relates to a set of other different but related constructs and their measures in the way that is expected. It entails assessing the theoretical relationship between different constructs and the observed relationships between construct indicators or measures, usually through evaluations based on formal hypotheses (Peter, 1981). SEM is one method to provide evidence of nomological validity and is used in conjunction with convergent validity results to establish construct validity; when a construct has been used in a prior study the indicator weights are compared (Cenfetelli & Bassellier, 2009). No evidence was found that the virtue ethics based ISS constructs used in the TWEB model have been utilized in prior studies, therefore tests for nomological network effects were not possible.

Discriminant validity is the extent that a construct is distinct from other constructs. This is indicated by showing that none of the construct indicator items are related to or measures another construct, thereby implying unidimensionality (Gefen & Straub, 2005; Kline, 1998; Peter, 1981). Issues are evident when indicators correlate more highly with indicators of constructs other than those of their parent construct. This means that the construct may be better explained by the indicators of a different construct rather than by its own observed indicators (Fornell & Larcker, 1981; Hair et al., 2009; Peter, 1981). AVE is also used as the basis to measure discriminant validity. If the squared correlation between two constructs is less than either of their individual AVEs it suggests that the constructs each have more internal variance than the variance shared between the constructs. If this is true for the target construct and all the other constructs it indicates discriminant validity of the target construct (Hair et al., 2012; MacKenzie et al., 2011). Indicator convergent and discriminant validity were also tested for cross-loading issues to ascertain whether any indicators warranted removal. Gefen and Straub recommend that indicators be checked for cross-loading, where an indicator loads higher on another construct other than its theoretically assigned construct, and they recommend considering the removal of any problematic indicators.

Cenfetelli and Bassellier (2009) recommend testing formative constructs indicators for low loadings and path weight, and if found then the researcher should investigate the contribution of those low scoring indicators to the construct to determine if they should remain in the construct set. Chin (2010) and Hair, (2011, 2012) report that the primary criteria for assessing an indicators contribution to its related construct is by indicator weight. The validity of formative constructs were evaluated by looking at the path weights going from each item to the constructs as well as cross-loadings between items and other constructs. Bootstrapping is the statistical method used to evaluate the stability of estimates or weights in PLS and establish confidence intervals (Chin, 2010; Hair et al., 2011). Hair et al. (2011, 2012) recommend that 5000 is the minimum number of samples for conducting bootstrap analysis.

Kurtosis and Skew

Data normality is identified through kurtosis and skew. Kurtosis describes the distribution of the data around the mean, measuring whether the data is peaked or flat compared to a normal distribution curve. A data set with high kurtosis tends to have a distinct peak near the mean, declines rapidly, and has heavy tails. Data sets with low kurtosis tend to have a flat top near the mean (Kline, 1998; Terrell, 2012). Skew is a measure of the symmetry of the data distribution. A data set is symmetric and considered normal if it looks the same on the left and right of the mean. Positive skew has the majority of the data below or to the right of the mean; negative skew has most of the data located above or to the left of the mean (Kline, 1998; Schumacker & Lomax, 1996; Terrell, 2012). Skewness and kurtosis values are each zero in a normal distribution; the further the value of their score on either the positive or negative side of zero the more non-normal the distribution. Kline (1998) notes that values of 3.0 and greater indicate extreme skewness; however, that the values for kurtosis (proper) are more arbitrary, ranging from 8.0 to 20, and recommends using a compromise value of 10 with increasing values indicating more serious normality issues. Terrell states skewness values exceeding 2 are problematic. Kim (2013) recommends for sample sizes greater than 300, a skew value larger than 2 and a kurtosis value larger than 7 should be used as threshold values for determining substantial non-normality.

Cronbach's alpha

Reliability testing in CFA provides evidence that indicators of a construct are in fact related to each other. One of the most popular statistics for determining reliability is Cronbach's alpha, an internal consistency test which measures the degree that indicators measure their associated latent construct and how closely related a set of items are as a group. It is also commonly used to determine the average correlation of items in a survey instrument to gauge its reliability (Tavakol & Dennick, 2011). Brown (2011) concurs, recommending that Cronbach's alpha should be used when checking the reliability of Likert scales. Reliability checks to determine if indicators are related is generally only applicable for reflective constructs; it is of little value to perform this reliability test on formative constructs as their measures are not correlated with each other. However, for models that have a mixture of formative and reflective constructs the use of Cronbach's alpha to test the reliability of the reflective constructs is desirable (Petter et al., 2007). In this research Cronbach's alpha was conducted on the four ISS virtue ethics constructs of the TWEB measurement model in order to provide support they were correctly identified as formative, and to establish reliability of the model's three reflective constructs. A low correlation between items adds strength to the assertion that the constructs are correctly identified as formative while high correlations may indicate that the constructs are either reflective or formative (MacKenzie et al., 2005). Values from 0 to 1 are used to describe the reliability of factors extracted from questions with two or more possible answers with a higher score indicating that reliability. Coefficients with values of 0.9 are considered excellent, 0.8 good, and 0.7 as adequate by Kline (1998); and 0.8 to 0.9 as acceptable by Salkind (2009).

In early stages of research new measures under development can be accepted with an alpha value of 0.60; otherwise, 0.70 should be the threshold according to Nunnally and Bernstein (1994). Tavakol and Denniick (2011) caution that if the alpha value is too high, such as 0.95, it suggests that some test items may be redundant as they are testing the same question in a different form and recommend a maximum value of 0.9. Measurement items which have a low correlation to a construct are typically dropped from the scale of a reflective model (Kline, 1998).

Inter-rater Agreement and Test-retest

Reliability is the extent to which an indicator or set of indicators are consistent in what they are intended to measure (Straub et al., (2004). If multiple measurements are taken, the reliable measures will all be very consistent in their values. Assessment of a set of indicators for reliability at the construct level is not applicable for first order formative constructs because it cannot be predicted that an indicator will be correlated with others. The correlation between each indicator could be positive, negative, or nonexistent, therefore attempting to establish reliability based on internal consistency may result in elimination of an indicator that was in fact key to the meaning of the construct (MacKenzie et al., 2011). Formative or causal indicators help to form a construct's conceptual meaning; therefore the relationship between a construct and indicators should be carefully considered prior to removing indicators solely based on score (Bollen &

Lennox, 1991). Research by Diamantopoulos and Winklhofer (2001), Mackenzie, Podsakoff, and Jarvis (2005), and MacKenzie et al. (2011) concluded that for constructs with formative indicators Cronbach's alpha is not an effective measure of reliability and recommend using test-retest or inter-rater reliability procedures.

Inter-rater reliability is established by evaluating the level of agreement between different raters regarding an indicator being measured (LeBreton & Senter, 2008; Mackenzie et al., 2011). The within-subject (indicator) standard deviation (SD) is the variability of the repeat measurements within the same subject scores used to capture the error of the outcome. It is desirable that the within-subject SD is small to indicate reliability (MacKenzie, Podsakoff, & Podsakoff, 2011).

Test–retest reliability is the variation in the measurement of an indicator as evaluated by a single person under the same conditions at two different points in time. It is expressed as the difference between the test and the retest measurement scores of same subjects. The correlation coefficient between test-retest measures provides an indication of whether the indicator is expected to be stable over time as well as an indication of the strength and reliability of the indicators that form the construct (MacKenzie et al., 2011; Petter et al., 2007). Straub et al. (2004) note that inter-rater agreement and test-retest are also used to demonstrate the reliability of reflective constructs.

For the formative and reflective constructs in this study's measurement model test-retest and inter-rater agreement were used to evaluate reliability. The interval used between the survey and the repeat survey is dependent on the purpose of the study and how the results are to be used (Salkind, 2009). The interval used in this study was 30 days, which is consistent with a similarly designed example survey by Leedy and Ormrod (2005).

Correlation Coefficient

The relationship between the test re-test results was evaluated by examining the correlations between variables using coefficient of correlation, also known as Pearson’s r. This procedure is widely used as a measure of the strength of the relationship and the degree of linear dependence between two variables, providing a goodness of fit indication of the relationship between them. Correlation direction values range from between +1 and −1, with 1 being total positive correlation, 0 being no correlation, and −1 being total negative correlation (Lind, Marchal, & Wathen, 2008; Sekaran & Bougie, 2010; Terrell, 2012). Correlation strength values between 0.8 and 1.0 are considered very strong, between 0.6 and less than 0.8 as strong, between 0.4 and less than 0.6 as acceptable, between 0.2 and less than 0.4 as weak and unacceptable , and less than 0.2 as very weak and unacceptable (Lind et al., 2008; Salkind, 2009).

Multicollinearity

Formative constructs should be assessed for multicollinearity, where two or more indicators are highly correlated - indicating conceptual overlap. While multicollinearity is desirable for reflective constructs, excessive multicollinearity in formative indicators can cause misinterpretation of the importance of the indicators or destabilize the construct (Cenfetelli & Bassellier, 2009; Jarvis et al., 2003; Petter et al., 2007). Large correlation coefficients in the correlation matrix of indicator items indicate multicollinearity. A high degree of multicollinearity is a value of 0.9, a value of 0.8 is considered moderate, and a value of less than 0.6 is considered good (Cenfetelli & Bassellier, 2009). Kline (1998) suggests correlation values as high as 0.85 are the indication of redundancy and identifies Variance Inflation Factor (VIF) as the alternate method of identifying multicollinearity issues; however, it is generally accepted that when all correlations are 0.7 or lower then there is no need to calculate VIF or eigenvalues.

Table 7, Measurement Model Analysis Procedures, summarizes the indices used to test the formative and reflective constructs of the TWEB measurement model. A summary of the fit index significance levels that were used in the evaluation of the measurement model is provided in Table 8.

Table 7: Measurement Model Analysis Procedures

Procedure	Constructs with Formative Indicators	Constructs with Reflective Indicators
Measurement model goodness of fit	X^2/df, RMSEA, SRMR, CFI, NNFI	X^2/df, RMSEA, SRMR, CFI, NNFI
Data set normality	kurtosis, skew	kurtosis, skew
Convergent validity	n/a	AVE Item to total correlation
Discriminant validity	Indicator weights bootstrap confidence interval	Inter-construct (squared) correlation
Reliability of indicator sets at the construct level	Cronbach’s alpha (only used to confirm formative nature of construct)	Cronbach’s alpha
Individual indicator Validity	Indicator weight cross-loading	Cross-loading
Individual indicator Reliability	Inter-rater agreement and test-retest Coefficient correlation	Inter-rater agreement and test- retest Coefficient correlation
Correlation between indicators	Multicollinearity	n/a

Table 8: Summary of Fit Index Significance Levels for Measurement Model

Test	Fit Index	Acceptable Fit Value	Reference
Model Fit	Relative (normed) chi-square (X^2/df)	1.0 to 5.0 2.0 to 5.0	Schumacker & Lomax (1996) Hooper et al. (2008)
Absolute Model Fit	RMSEA	≤ 0.05 is good fit 0.05 to 0.08 is reasonable fit ≤ 0.06 is good fit	Dow et al. (2008); Schreiber et al. (2006); Schumacker & Lomax (1996) MacKenzie et al. (2011)
Absolute Model Fit	SRMR	< 0.05 is well fitting ≤ 0.08 is acceptable fit	Hooper et al. (2008) MacKenzie et al. (2011); Schreiber et al. (2006)
Relative Model Fit	CFI	0.90 is acceptable, ≥ 0.95 for good fit ≥ 0.95 for acceptance	Hooper et al. (2008 MacKenzie et al. (2011) Schreiber et al. (2006)
Relative Model Fit	NNFI	≥ 0.95 for acceptance 0.90 reflects good fit	Hooper et al. (2008, Schreiber et al. (2006) Schumacker & Lomax (1996)
Convergent and Discriminate Validity	AVE Item to total correlation Factor-indicator loading Indicator loading & weight Cross-loading Squared correlation	≥ 0.50 is acceptable ≥ 0.30 is acceptable ≥ 0.70 is acceptable ≥ 0.50 is acceptable Determined by number of indicators Loads highest on assigned construct is acceptable AVE > than squared correlation AVE	Gefen & Straub (2005); Hair et al. (2009; 2012) Nunnally & Bernstein (1994) Straub et al. (2004) MacKenzie et al. (2011) Cenfetelli & Bassellier (2009) Gefen & Straub (2005) MacKenzie et al. (2011)

Table 8: Summary of Fit Index Significance Levels for Measurement Model (continued)

Test	Fit Index	Acceptable Fit Value	Reference
Normality	Kurtosis	< 10 ≤ 7	Kline (1998) Kim (2013)
	Skew	< 3 ≤ 2	Kline (1998) Kim (2013; Terrell, 2012)
Reflective Construct Reliability	Cronbach's alpha	≥ 0.70 is adequate, 0.8 is good, 0.9 is excellent	Kline (1998)
		0.8 to 0.9 is acceptable	Salkind (2009)
		0.9 is acceptable	Tavakol & Denniick (2011)
		≥ 0.60 is acceptable for new	Nunnally & Bernstein (1994)
Formative and Reflective Construct Reliability	Inter-rater agreement	Low standard deviation	LeBreton & Senter, (2008); MacKenzie et al. (2005, 2011); Petter et al., (2007)
	Test-retest (using correlation coefficient)	0.8 to 1.0 = very strong 0.6 to < 0.8 = strong 0.4 to < 0.6 = acceptable 0.2 to < 0.4 = weak 0.0 to < 0.2 = very weak (0 to 0.4 = unacceptable)	Lind, Marchal, & Wathen (2008); Salkind, (2009)
Collinearity	Multicollinearity	< 0.80 is acceptable	Cenfetelli & Bassellier (2009)

Evaluation of Structural Model

In the SEM phase the structural or inner model's structural relationships and validity were evaluated using PLS-SEM. The primary objective of PLS-SEM is to maximize the explained variance in the dependent variables. An overview of the methods selected for use in evaluating the structural model follows.

Chin (2010), Hair, (2011, 2012), and MacKenzie et al. (2011) report that the primary criteria for assessing a formative construct is by R^2 and path weight. A shortcoming of the statistical analysis software package used by “R” for PLS, PLSPM, does not report R^2 for formative constructs. Therefore, the validity of the formative constructs in the TWEB inner were evaluated by looking at path weights between each construct to other constructs as recommended by Cenfetelli and Bassellier (2009), Chin (2010), and Hair (2011, 2012).

Path Weight

The path weight or effect size is an estimate of a population parameter based on a sample. Effect size, the practical or substantive significance, refers the magnitude and direction of the difference between two groups or the strength of the relationship between two variables (Schumacker & Lomax, 1996). The effect size is the main finding of a quantitative study. The acceptable fit points for effect sizes are somewhat arbitrary, in regression and SEM, standardized path weights less than 0.10 are considered small effects, around 0.30 as medium effects, and 0.5 or more as large effects (Kline, 1998). Chin (2010) is less specific, identifying a value of 0.05 as small and 0.10 as significant. Inner model parameters in PLS are non-significant at less than 0.10 according to Tenenhaus (2008). Regardless of which value is used, the most important output of a research study should be one or more measures of effect size as it quantifies the size of the difference or strength of the relationship, not *p*-values (Chin, 2010; Coe, 2002).

p-value

The *p*-value, or statistical significance, measures the strength of the evidence or power to support the null hypothesis by comparing the statistical value obtained to a critical value. The acceptable value of the path weight is based on the significance of the sample size. Sample sizes are important to research as they provide precision and confidence in the results; and large samples - defined as 200 to 400, tend to be more significant and are required for SEM (Kline, 1998). Schumacker and Lomax (1996) suggest that samples consisting of between 5 and 10 responses per model variable are sufficiently large depending on the type of distribution. The TWEB model has a total of 42 variables, 7 of which are latent – the 4 formative and 3 reflective constructs. Three indicator items were removed at the measurement model stage, specifically indicators II1, II3, and EB5; leaving 35 manifest variables. The survey produced 395 complete responses; falling in the range of each of the cited definitions as being a large sample.

If a path weight – the effect size - is identified as being statistically significant, meaning distinguishable from a particular number -usually zero, it means that there is confidence, typically at 95%, that the particular path weight is not zero. The *p*-value is a number between 0 and 1; with values ≤ 0.05 indicating strong evidence against the null hypothesis, values > 0.05 indicating weak evidence against the null hypothesis, and values close to 0.05 considered marginal; however, interpreting a particular *p*-value as support should vary with the hypothesis (Schervish, 1996). According to Kline (1998) the level of significant depends on what the researcher chooses, with less than 0.05 or 0.01 being typical. Leedy and Ormrod (2005) state that setting a significance level is a balancing act, too low increases the likelihood of a Type I error, and too high increases the probability of a Type II error, and recommend .05 as a trade-off point. Lind et al. (2008) states that values greater than 0.1 provide some evidence not to reject, values of 0.05 strong evidence not to reject, and 0.01 very strong evidence not to reject.

A *t*-test determines statistical differences between two means (Salkind, 2009). The *p*-value reported with a *t*-test represents the probability of error involved in accepting a hypothesis when the population standard deviation is not known as the *t*-test distribution is more spread out than that of a normal distribution.

While a *p*-value can inform whether an effect exists, it will not reveal the size of the effect. A research study can obtain significant results by either have a very large sample size with small effects, or by having a small sample size with very large effects (Coe, 2002). In reporting and interpreting studies, both the effect size and statistical significance (*p*-value) are essential results to be reported. Table 9 provides a summary of the fit index significance levels that were used in the evaluation of the structural model.

Table 9: Summary of Fit Index Significance Levels for Structural Model

Test	Fit Index	Acceptable Fit Value	Reference
Model Fit	Path weight	≤ 0.10 = small 0.30 = medium ≥ 0.50 = large	Kline (1998)
		0.05 = small ≥ 0.10 = significant	Chin (2010)
		≥ 0.10 = significant	Tenenhaus (2008)
Hypothesis testing	*p*-value	≤ 0.05 = reject null hypothesis > 0.05 = do not reject null hypotheses	Leedy & Ormrod (2005)
		< 0.05 or < 0.01 depending on level chosen	Kline (1998)
		> 0.1 = some evidence not to reject .05 = strong evidence not to reject .01 = very strong evidence not to reject	Lind et al. (2008)

There are many indices used in SEM to measure overall or average fit, and any one index can be good even if its fit in one portion of the model is bad. Furthermore, good values do not guarantee that the model makes theoretical sense and do not prove that the model under study is correct. Researchers must take care in selecting the indices used for model fit testing and assessment and not make the error of selecting the indices used just because those indices best fit the model data (Barrett, 2007). The indices selected to report the results of this study were based on their perceived effectiveness and accuracy as reported by previous research, and while an individual index may not provide a best fit, when looked at as a set should provide an accurate assessment of the TWEB theoretical model.

3.6 Miscellaneous

This section details the resource requirements and assumptions of the research study.

Resources that were required to complete this study included:

- ten expert panel members with the CISSP credential
- 30 pilot study participants consisting of ICT, ISS, and administrative professionals
- Approximately 400 survey participants from an ISS professional organization
- Statistical analysis software
- Web survey hosting service

The assumptions of this study have been detailed throughout Chapter 3 and are summarized in Table 10, Research Study Assumptions.

Table 10: Research Study Assumptions

1	An information system, the combination of Information Computing Technology and human activities that support operations, is considered an infosphere.
2	The Information Ethics model as presented by Floridi (1999, 2006) has been accepted by the research community as a valid ethical model.
3	The factors that shape a moral agents moral and ethical deliberations are not identified or included as part of Floridi's (1999, 2006) infosphere, the information system.
4	The infosphere authoritative organization is acting morally – doing the right thing.
5	The concept of Virtue Ethics is derived from the four cardinal virtues of temperance, fortitude, prudence, and justice as defined by Aristotle (2005) and Aquinas (2005).
6	Sample size requirements do not increase much for populations of more than 20,000

3.7 Summary

This chapter described the theoretical foundation for this study and presented the research methodology which was used. Information gathered from the literature review regarding virtue ethics, IS security, security cultures in organizations, trusted workers, and failures of technical controls, policies, and procedures was considered when developing this research framework. This study builds upon the research and theories of Floridi (2006) regarding Information Ethics (IE), modifying and extending Floridi's IE model to be more aware and inclusive of influences on information that affect the ethical choices of moral agents who are identified as IS workers in trusted positions. The revised

IE model incorporates the new category of info-influencer. This new category is comprised of ISS Virtue Ethics based constructs, factors which affect the actions of a moral agent. This study also draws on the research of Weber (1981, 1993, 2010) regarding institutionalizing ethics into business organizations. A new conceptual model was proposed, the ISS Trusted Worker Ethical Behavior Model, which is comprised of virtue ethics based ISS trusted worker ethical constructs, influences, and reflected behavior. This model extends existing research and is useful in identifying important factors that influence the actions of a moral agent and ultimately affect information system security.

Previous research conducted through literature reviews, expert panels, and surveys was used to develop the proposed constructs was summarized. The use of the survey methodology to gather quantitative data to further develop, validate, and test the reliability of the proposed constructs and the theoretical model through CFA and SEM were described. Issues related to population and sample selection, statistical techniques to be used, and data collection and analysis were discussed. The procedure for establishing the statistical significance of the results was delineated. Resources required to conduct the research study and assumptions were presented.

Chapter 4

Results

4.1 Introduction

Following the guidelines by Diamantopoulos (2011), Jarvis et al. (2003), MacKenzie et al. (2011), Petter et al. (2007), and Schreiber et al. (2006) the TWEB model constructs and indicators were categorized as either formative or reflective. Because the TWEB model contains both formative and reflective constructs, use of only covariance based global fit indicators in the CFA phase was not appropriate. It was also necessary to employ component based fit tests for the formative construct portions of the model. Traditional global fit indicators were used in the CFA of the reflective constructs.

4.2 Data Analysis

4.2.1 Demographic Data

Section One of the survey instrument, Appendix B, collected demographic data of the survey participants in order to establish external validity of the sample results and assurance in them being SMEs in the field of Information Assurance (IA) and ISS. This was necessary as the sample must be representative of the population in order to provide useful, accurate answers to the survey questions and to establish confidence in the accuracy of the data collected (Sekaran & Bougie, 2010). Demographic information regarding each participant's ISS education and experience was collected. It was deemed by the researcher that age and gender data was not relevant to the study's focus, therefore this information was not collected. The demographic data of the participants is shown in Table 11.

Table 11: Survey Participant Demographic Data

Professional Characteristic	Frequency	Percentage
Employed directly in ISS field: Yes	344	78.0
No	97	22.0
Total	441	100.0
Professional Roles:		
C-level Executive	42	9.5
Information Assurance Manager/Officer	52	11.8
IT Department, Division Head, Manager	41	9.3
Information Assurance/Security Specialist	137	31.1
IT Specialist	55	12.5
IA/IS/IT Student	14	3.2
Other	100	22.7
Highest Level of Education:		
Some High School	0	0
High School Graduate	12	2.7
Some College (no degree)	40	9.1
Associate Degree	39	8.8
Bachelor's Degree	128	29.0
Advanced Degree	194	44.0
Other	28	6.3
Degree Major:		
IA/IS/IT or Computer Field	246	55.8
Other	144	32.7
N/A	51	11.6
Years of ISS Experience:		
(Rounded up or down as necessary) 0-5	99	22.4
6-10	90	20.4
11-15	105	23.8
16+	147	33.3
Holds a Professional IS Security Certification:		
Yes	280	63.5
No	161	36.5

While incomplete surveys were included in the calculation of the survey response rate for demographics, the available responses on the incomplete surveys were not included in the data analysis.

The range of the relevant characteristics of professional roles, education, experience, and certifications are well represented by this surveys participants and correspond closely with sample populations of other IS studies; providing confidence about the representativeness of the sample. Additionally, the expertise of the survey participants in the field of IA and ISS appears to be confirmed and they are considered to be an accurate representation of the population they are intended to represent.

4.2.2 Measurement Model Data Analysis Results

The results of the confirmatory factor analysis of the measurement or outer model are organized by the analysis procedure and the fit indices that support them. Details regarding the specific indices and cutoff values chosen for reporting the measurement model data analysis results are discussed in Section 3.5.4, Data Analysis. The TWEB model was tested for goodness of fit, data set normality, and parsimony. Results are as follows:

Goodness of Fit

Goodness of fit describes how well a model fits a set of observations. Several goodness of fit statistical tests were used to determine how well the TWEB model reflective constructs fit the data collected.

Relative Chi-square X²/df was used to check for over identified models and models that do not fit the observable data. An acceptable fit value ranges from 1.0 to 5.0. RMSEA was used to assess the absolute fit of a measurement model; acceptable fit values are less than 0.06 being good and between 0.06 and 0.08 as being reasonable. SRMR was used to assess absolute fit; it is a measure of the mean absolute correlation residual, the overall difference between the observed and predicted correlations. Acceptable fit values are less than 0.05 being well fitting and up to 0.08 as acceptable. CFI was used to check the extent to which the target model was better than that of the null model. Acceptable fit values are 0.90 or greater. NNFI is an incremental measure of goodness of fit that compares a target model to a baseline or null model. Acceptable fit values are 0.90 or greater. A summary of the goodness of fit results for the reflective portion of the TWEB model are listed in Table 12.

Table 12: TWEB Outer Model Goodness of Fit Results

Index	Acceptable Fit Value	Actual Fit Value	Fit
χ^2/df	1.0 to 5.0	205.524/73.0 = 2.84	good
RMSEA	≤ 0.08	0.068	acceptable
SRMR	≤ 0.08	0.052	acceptable
CFI	≥ 0.90	0.909	acceptable
NNFI	≥ 0.90	0.886	marginally unacceptable

The reflective constructs were also individually tested for goodness of fit. Results are detailed in Table 13.

For all three constructs the χ^2/df, RMSEA, and NNFI fit was poor, for all three constructs the SRMR and CFI fit was acceptable.

Table 13: Reflective Construct Goodness of Fit Results

Construct	Construct Identifier	χ^2/df	RMSEA	SRMR	CFI	NNFI
Ethical Behavior	EB	7.76 poor fit	.131 poor fit	.045 good fit	.925 good fit	.775 poor fit
External Influences	EI	9.97 poor fit	.151 poor fit	.059 good fit	.899 good fit	.831 poor fit
Internal Influences	II	5.17 poor fit	.117 poor fit	.043 good fit	.934 good fit	.802 poor fit

Data Set Normality

Statistical tests and procedures in research assume that a data set has a normal distribution. Results obtained which assume normal distribution of data when this assumption is in fact not valid could result in incorrect conclusions. Kurtosis and skew were the two tests conducted to determine the normality of the data collected in this study.

Kurtosis and Skew

Kurtosis is a measure of whether the data is peaked or flat relative to a normal distribution. Positive kurtosis indicates a peaked distribution and negative kurtosis indicates a flat distribution. The acceptable threshold for kurtosis used was 7 or less. Skew is a measure of the lack of symmetry in the distribution of a data set. The distribution of the data set is symmetric if it looks the same to the left and right of the center point. The skew for a normal distribution is zero. Negative values for skewness indicate data that is skewed left while positive values for skewness indicate data that is skewed right of the center point. The acceptable range for skew used was between -2 to 2.

Significant kurtosis and skew would indicate that the data distribution is not normal. The standard error of kurtosis and skew reflect the precision of the estimate.

It should be noted that kurtosis and skew are measures better suited for reporting on continuous variables rather than categorical variables such as nominal, dichotomous, or ordinal. The variables in this study are ordinal as is typical for Likert-type scales, and fall in between continuous and categorical for statistical suitability. Some researchers consider frequencies and percentages more informative for ordinal items, therefore the response frequency and percentage information for each survey item is included in Appendix E.

The kurtosis and skew for each variable is presented in Table 14. The values are within the acceptable ranges that were established in Chapter 3, and indicate that the data is normally distributed.

Table 14: Kurtosis and Skew

Observable Indicator Identifier	Kurtosis		Skew	
	Statistic	Std. Error	Statistic	Std. Error
AS1	4.453	.240	-1.953	.120
AS2	1.645	.240	-1.023	.120
AS3	5.454	.240	-1.819	.120
AS4	5.441	.240	-1.848	.120
AS5	2.688	.240	-1.474	.120
AS6	2.339	.240	-1.198	.120
AS7	1.527	.240	1.205	.120
AS8	.552	.240	-1.035	.120
CO1	-.165	.243	-.674	.122
CO2	2.961	.243	-1.198	.122
CO3	1.487	.243	1.429	.122
CO4	2.064	.243	-.831	.122
CO5	1.501	.243	-.910	.122
RE1	.090	.244	.670	.122
RE2	3.456	.244	1.697	.122

Table 14: Kurtosis and Skew (continued)

Observable Indicator Identifier	Kurtosis		Skew	
	Statistic	Std. Error	Statistic	Std. Error
RE3	1.914	.244	-1.137	.122
RE4	3.954	.244	1.852	.122
RE5	.726	.244	-1.050	.122
SD1	2.539	.244	1.472	.122
SD2	2.978	.244	-1.387	.122
SD3	1.822	.244	-.946	.122
II1	1.393	.245	-.621	.123
II2	4.005	.245	1.534	.123
II3	.823	.245	-.950	.123
II4	1.447	.245	1.001	.123
II5	4.686	.245	1.680	.123
EI1	1.621	.245	-1.144	.123
EI2	2.619	.245	-1.161	.123
EI3	.313	.245	.918	.123
EI4	.951	.245	.860	.123
EI5	3.874	.245	-1.281	.123
EI6	4.154	.245	-1.181	.123
EI7	3.812	.245	-1.074	.123
EB1	.249	.245	-.602	.123
EB2	-.298	.245	-.922	.123
EB3	-.487	.245	-.372	.123
EB4	2.135	.245	-1.079	.123
EB5	-.595	.245	.641	.123

Convergent Validity

Tests for convergent validity were not conducted on the TWEB model formative constructs as prior research indicates it is not appropriate. For the reflective constructs, convergent validity was evaluated using average variance extracted (AVE) to determine inter-item correlation. AVE was assessed for each reflective construct with 0.50 used as the acceptable fit value. A small item-correlation provides evidence that the item is not measuring the same area as measured by the other items in the construct set. A correlation value of less than 0.2 or 0.3 indicates that the corresponding item does not correlate very well with the scale overall and therefore it may be dropped as recommended by Kline (1998). An item to total correlation cutoff value of 0.30 was used.

For the Ethical Behavior construct the measure for convergent validity, AVE, was less than the conventionally acceptable value of 0.5. Additionally, the low item to total correlation for item EB5 indicates that it was a candidate for removal from the indicator set although the cutoff value does fall within the accepted range of some researchers. All other items meet the accepted cutoff value and thus are considered valid items that represent the Ethical Behavior construct. Details are presented in Table 15.

Table 15: Ethical Behavior Construct Inter-Item Correlation Matrix

AVE	Identifier	EB1	EB2	EB3	EB4	EB5
.469	EB1	1.000	.358	.316	.344	.026
	EB2	.358	1.000	.104	.301	.222
	EB3	.316	.104	1.000	.321	.053
	EB4	.344	.301	.321	1.000	.133
	EB5	.026	.222	.053	.133	1.000
	Item to Total Correlation	.409	.397	.359	.440	.260

For the External Influences construct the AVE was acceptable. Additionally, all indicator items met the accepted cutoff value and are therefore considered valid items that represent the construct. Details are presented in Table 16.

Table 16: External Influences Construct Inter-Item Correlation Matrix

AVE	Identifier	EI1	EI2	EI3	EI4	EI5	EI6	EI7
.502	EI1	1.000	.595	.366	.385	.351	.357	.498
	EI2	.595	1.000	.315	.430	.367	.442	.455
	EI3	.366	.315	1.000	.483	.302	.289	.320
	EI4	.385	.430	.483	1.000	.444	.344	.387
	EI5	.351	.367	.302	.444	1.000	.554	.548
	EI6	.357	.442	.289	.344	.554	1.000	.554
	EI7	.498	.455	.320	.387	.548	.554	1.000
	Item to Total Correlation	.594	.611	.480	.583	.577	.574	.637

The AVE for the Internal Influences construct was acceptable. The low item to total correlation for indicator items II1 and II3 indicates that they were candidates for removal from the set. All other items met the accepted cutoff value and thus are considered valid items that represent the Internal Influences construct. Details are presented in Table 17.

Table 17: Internal Influences Construct Inter-Item Correlation Matrix

AVE	Identifier	II1	II2	II3	II4	II5
.573	II1	1.000	.225	.167	.083	.018
	II2	.225	1.000	.038	.363	.407
	II3	.167	.038	1.000	.112	.028
	II4	.083	.363	.112	1.000	.339
	II5	.018	.407	.028	.339	1.000
	Item to Total Correlation	.195	.419	.130	.366	.316

Items EB5, II1, and II3 were subsequently removed from further analysis in order to improve the covariance based portion of the measurement model fit.

Discriminant Validity

Discriminant validity can be verified by comparing the AVEs with correlations between the latent variables. For the three reflective constructs of Ethical Behavior, External Influences, and Internal Influences used in this analysis, the squared-correlation between the latent variables was smaller than the respective AVEs for the constructs, suggesting acceptable discriminant validity. Results are displayed in Table 18.

Table 18: Correlations between Latent Variables

Latent variable	Astuteness	Conviction	Rectitude	Self-Discipline	Internal influences	External influences	Ethical behavior
Astuteness	1.000	.463	.415	.287	.354	.340	.340
Conviction	.463	1.000	.483	.482	.387	.351	.372
Rectitude	.415	.483	1.000	.410	.382	..385	.447
Self-Discipline	.287	.482	.410	1.000	.334	.330	.446
Internal influences	.354	.387	.382	.334	1.000	.529	.262
External influences	.340	.351	.385	.330	.529	1.000	.351
Ethical behavior	.340	.372	.447	.446	.262	.351	1.000

For formative constructs, convergent validity, and construct reliability cannot be assessed in the same manner as reflective constructs. For formative constructs, items are no longer realizations of the latent construct but rather its facets. Each item thus represents a part or dimension of the latent formative construct that is not necessarily captured by other items. Items defining formative constructs may or may not correlate with each other (Jarvis et al., 2003), and unlike the case for reflective constructs, Cronbach's alpha and AVE are not appropriate or logical tests for assessing formative constructs (Bollen & Lennox, 1991).

Alternatively, path weights are used to assess the importance of each indicator comprising a particular formative construct. Removing specific items from the measurement model should also be attempted with extra care because items are assumed to capture different aspects of the construct; therefore removing an item could result in the loss of information not captured by the other indicators of the construct (Cenfetelli & Bassellier, 2009). Bootstrapping was performed on 5000 samples to determine the

Table 19: Summary of Outer Model and 95% Bootstrap Confidence Intervals

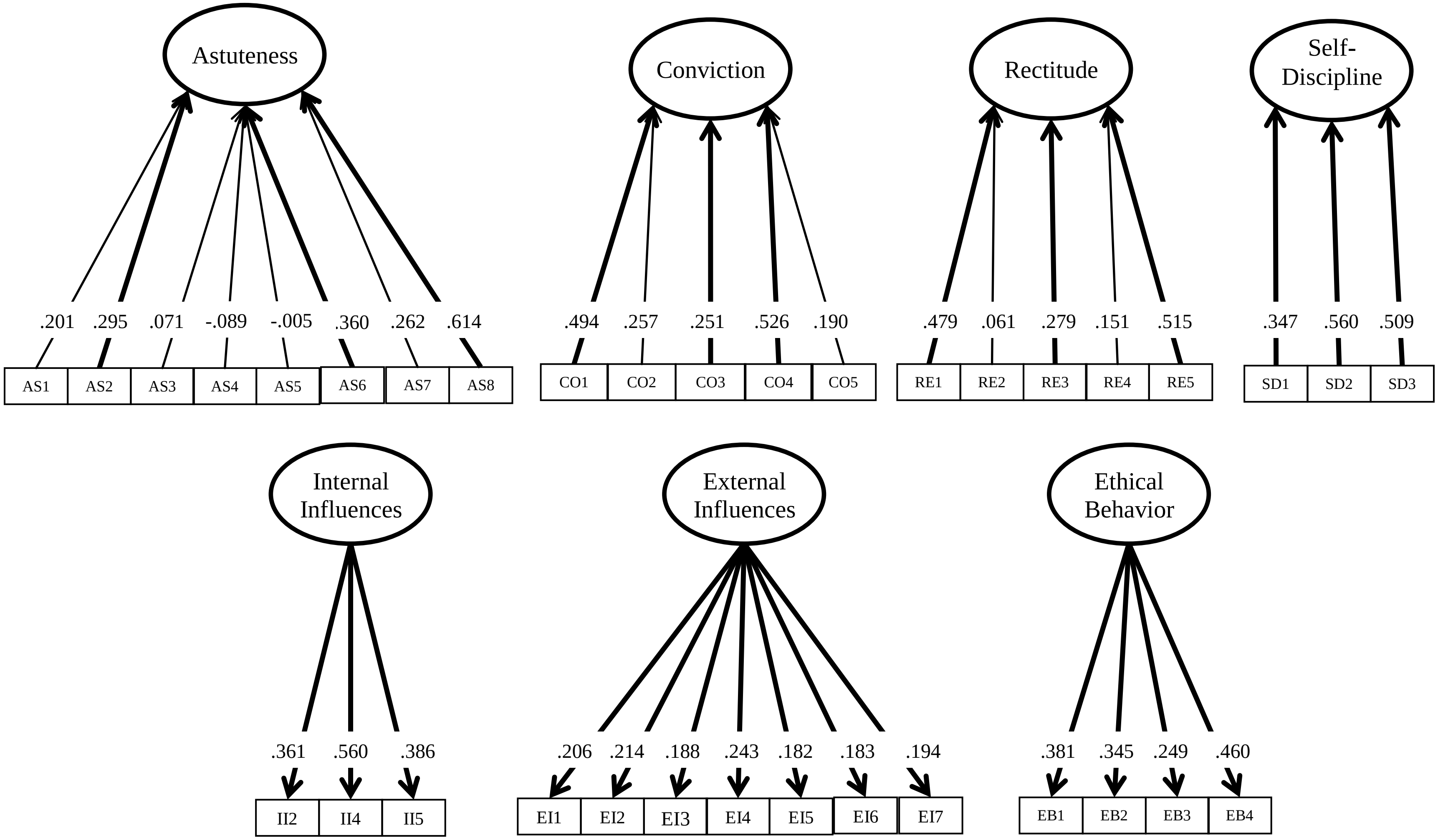
Construct Identifier	Path Weight	Standard Error	Lower	Upper	Loading	Communality
AS1	.201	.141	-.089	.422	.413	.170
AS2	.295	.129	.059	.536	.480	.231
AS3	.071	.135	-.158	.310	.359	.129
AS4	-.089	.161	-.334	.299	.203	.041
AS5	-.005	.126	-.271	.226	.236	.056
AS6	.360	.135	.079	.592	.597	.357
AS7	.262	.131	-.035	.464	.498	.248
AS8	.614	.117	.309	.731	.690	.477
CO1	.494	.145	.233	.765	.610	.372
CO2	.257	.164	-.073	.533	.629	.396
CO3	.251	.104	.071	.437	.384	.147
CO4	.526	.148	.226	.776	.677	.458
RE1	.479	.115	.204	.663	.751	.564
RE2	.061	.137	-.232	.353	.525	.275
RE3	.279	.110	.039	.461	.604	.365
RE4	.151	.118	-.064	.402	.455	.207
RE5	.515	.106	.322	.719	.720	.518
SD1	.347	.090	.172	.512	.432	.187
SD2	.560	.096	.398	.757	.814	.663
SD3	.509	.102	.286	.655	.774	.599
II2	.361	.069	.213	.492	.721	.520
II4	.560	.070	.434	.704	.822	.676
II5	.386	.061	.272	.498	.723	.522
EI1	.206	.026	.151	.244	.722	.521
EI2	.214	.026	.165	.269	.736	.542
EI3	.188	.033	.138	.267	.618	.382
EI4	.243	.033	.181	.316	.724	.525
EI5	.182	.032	.128	.237	.705	.497
EI6	.183	.028	.127	.235	.697	.486
EI7	.194	.027	.144	.238	.749	.561
EB1	.381	.032	.318	.448	.742	.550
EB2	.345	.043	.248	.411	.646	.417
EB3	.249	.039	.175	.319	.554	.307
EB4	.460	.041	.384	.534	.775	.601

statistical significance of each indicator weight and loading, with the results indicating support for retaining all of the indicators.

For the formative and reflective constructs in the TWEB model, the weights and respective standard errors as well as bootstrap confidence intervals are presented in Table 19. Some formative indicators, particularly AS3, AS4, AS5, and RE2 were not significant predictors of their respective construct; however, following the recommendation of Cenfetelli and Bassellier (2009) these items were retained in the model. In the cases of AS4 and AS5, if they repeatedly test negative they should be considered for rejection from the construct. The formative indicators of AS1, AS7, CO2, CO5, and RE4 were not strongly significant; however, this is likely a result of the constructs consisting of numerous indicators (Hair, 2011). All other weights were significant, providing empirical support that they should be retained.

A graphical representation of the PLS outer model displaying the TWEB model constructs and their respective indicators is shown in Figure 10. Thicker lines denote statistically significant path weights at $\alpha = .05$ and implies that these indicators are the most important to their respective construct as detailed by Chin (2010).

Figure 10: Outer PLS Model for Formative and Reflective Constructs



Reliability of Indicator Sets at Construct Level

Cronbach's alpha is based on the covariances among the items. Cronbach's alpha based on Standardized Items depends on the correlation among the items; it assumes that all of the items have equal variances. The higher the alpha is, the more reliable the item. When used to test formative constructs this index is only used to provide evidence to confirm their formative nature.

Cronbach’s alpha results for the entire measurement model are presented in Table 20. As noted in Chapter 3, this study used a fit value of 0.60 or higher to indicate reliability for newly developed items. The low Cronbach’s alpha scores for the constructs of Astuteness, Conviction, Rectitude, and Self-Discipline provides evidence that those four constructs are in fact formative versus reflective.

Table 20: Formative and Reflective Construct Reliability

Construct	Construct Identifier	Cronbach’s *a*	Cronbach’s *a* Based on Standardized Items
Astuteness	AS	.411	.493
Conviction	CO	.194	.268
Rectitude	RE	-.129	-.105
Self-Discipline	SD	.182	.216
External Influences	EI	.824	.961
Internal Influences	II	.633	.697
Ethical Behavior	EB	.592	.669

The reliability measure of the reflective construct of External Influences is acceptable, while the constructs of Internal Influences and Ethical Behavior are acceptable as new items using the recommended value of 0.6 per Nunnally and Bernstein (1994) and minimally unacceptable by researchers using 0.7 as the accepted level.

Individual Indicator Validity

Individual construct indicator loadings were evaluated to establish indicator validity. Table 21 displays the loadings and cross-loadings of all indicator items with all constructs. Reviewing down a particular construct column, loadings should be higher on a particular indicator than that of the cross-loadings. Going across a particular indicator row, an item should be more strongly related to its construct than any other.

All items load highest on their respective construct except in one case, where AS4 loads higher on Conviction than on Astuteness. Due to the formative nature of both constructs, this item was not removed from the analysis, however, it should be considered for further evaluation using the scale development process described by MacKenzie et al. (2011).

Individual Indicator Reliability

Inter-rater Agreement was one test used to evaluate the individual indicator reliability of the measurement model constructs. The within indicator or subject standard deviation (SD) is the variability of the responses of survey participants for each survey item. SD is used to assess how far the values are spread above and below the mean. A high SD indicates that the data is widely spread and less reliable, a low SD shows that the data are clustered closely around the mean and more reliable. The majority of items fell within one SD from the mean which implies good reliability of the construct indicators, only one item, RE5, demonstrated weak reliability on both scales. Future refinement of the indicator items and survey instrument per MacKenzie et al. (2011) may improve indicator reliability. Table 22 displays the Inter-rater Agreement Results.

Table 21: Indicator Item Cross-loadings

Variable	Astuteness	Conviction	Rectitude	Self-discipline	Internal influences	External influences	Ethical behavior
Astuteness							
AS1	.413	.317	.287	.172	.144	.097	.140
AS2	.480	.252	.207	.176	.156	.149	.163
AS3	.359	.234	.194	.177	.222	.159	.122
AS4	.203	.235	.185	.177	.156	.148	.069
AS5	.236	.201	.120	.152	.079	.015	.080
AS6	.597	.319	.275	.188	.215	.246	.203
AS7	.498	.362	.356	.199	.333	.268	.169
AS8	.690	.197	.175	.138	.184	.196	.235
Conviction							
CO1	.171	.610	.220	.258	.173	.155	.227
CO2	.383	.629	.360	.345	.247	.249	.234
CO3	.197	.384	.219	.196	.295	.235	.143
CO4	.341	.677	.332	.329	.210	.178	.252
CO5	.269	.443	.275	.229	.282	.303	.165
Rectitude							
RE1	.288	.341	.751	.258	.282	.253	.336
RE2	.290	.381	.525	.360	.447	.350	.235
RE3	.313	.308	.604	.306	.265	.327	.270
RE4	.165	.348	.455	.278	.328	.263	.204
RE5	.285	.307	.720	.266	.186	.216	.322

Table 21: Indicator Item Cross-loadings (continued)

				Self-	Internal	External	Ethical
Variable	Astuteness	Conviction	Rectitude	discipline	influences	influences	behavior
Self-discipline							
SD1	.203	.264	.288	.432	.411	.361	.193
SD2	.215	.364	.316	.814	.172	.169	.363
SD3	.189	.366	.262	.774	.188	.217	.345
Internal influences							
II2	.256	.301	.335	.239	.721	.446	.160
II4	.340	.297	.273	.303	.822	.395	.248
II5	.184	.290	.280	.203	.723	.381	.171
External influences							
EI1	.272	.278	.326	.227	.304	.722	.253
EI2	.220	.275	.302	.251	.372	.736	.262
EI3	.275	.250	.259	.184	.383	.618	.231
EI4	.270	.249	.263	.279	.440	.724	.298
EI5	.189	.167	.196	.232	.299	.705	.223
EI6	.209	.273	.269	.241	.417	.697	.224
EI7	.243	.241	.285	.212	.400	.749	.237
Ethical behavior							
EB1	.224	.295	.340	.333	.135	.243	.742
EB2	.260	.240	.269	.230	.179	.244	.646
EB3	.150	.149	.287	.279	.072	.093	.554
EB4	.277	.304	.333	.370	.285	.329	.775

Table 22: Inter-rater Agreement Results

Observable Indicator Identifier	Associated Survey Question	Mean	Standard Deviation	Retest Mean	Retest Standard Deviation
AS1	A-1	4.659	0.734	4.659	0.499
AS2	A-2	4.275	0.634	4.308	0.591
AS3	A-3	4.703	0.459	4.637	0.506
AS4	A-4	4.725	0.496	4.681	0.492
AS5	A-5	4.220	0.892	4.275	0.731
AS6	A-6	4.440	0.670	4.462	0.602
AS7	A-7	1.637	0.837	1.582	0.746
AS8	A-8	4.099	1.033	4.132	0.921
CO1	B-1	3.945	1.026	3.802	1.035
CO2	B-2	4.341	0.703	4.363	0.691
CO3	B-3	1.802	1.147	1.813	0.977
CO4	B-4	4.319	0.594	4.264	0.534
CO5	B-5	4.363	0.606	4.363	0.738
RE1	C-1	2.110	0.983	1.934	0.940
RE2	C-2	1.429	0.685	1.462	0.735
RE3	C-3	4.154	0.942	4.209	0.768
RE4	C-4	1.451	0.806	1.560	0.885
RE5	C-5	4.220	1.020	4.176	0.754
SD1	D-1	1.626	0.784	1.626	0.626
SD2	D-2	4.352	0.639	4.352	0.545
SD3	D-3	4.011	0.796	4.088	0.626
II1	E-1	3.923	0.582	3.978	0.614
II2	E-2	1.308	0.487	1.440	0.581
II3	E-3	3.626	0.902	3.758	0.861
II4	E-4	1.769	0.776	1.725	0.746
II5	E-5	1.363	0.624	1.473	0.544
EI1	E-6	4.088	0.812	4.198	0.749
EI2	E-7	4.121	0.814	4.231	0.651
EI3	E-8	1.758	0.779	1.879	0.828
EI4	E-9	1.989	0.782	1.956	0.773
EI5	E-10	4.308	0.662	4.319	0.612
EI6	E-11	4.495	0.545	4.473	0.621
EI7	E-12	4.297	0.641	4.308	0.627
EB1	F-1	3.945	0.835	4.044	0.698
EB2	F-2	3.385	1.428	3.198	1.400
EB3	F-3	3.198	0.909	3.495	0.808
EB4	F-4	4.275	0.731	4.341	0.562
EB5	F-5	2.110	1.140	2.209	1.131

Test-retest was another method used to evaluate the individual indicator reliability of the measurement model constructs. Correlations between test-retest data provides an indication of whether individual indicators are expected to be stable over time as well as an indication of the strength and reliability of the indicators that form the construct. Acceptable fit values are 0.8 to 1.0 being very strong, 0.6 to < 0.8 as strong, 0.4 to < 0.6 as acceptable, and 0.2 to < 0.4 as weak.

Thirteen of the survey questions were designed for reversed responses. They are identified in Table 23 with the observable indicator identifiers of AS7, CO3, RE1, RE2, RE4, SD1, II2, II4, II5, EI3, EI4, EB2, and EB5. The fact they were designed for reversed responses did not appear to be confusing to participants or affect them being answered incorrectly as 11 out of the 13 had an acceptable or higher coefficient correlation fit.

Seven observable indicator identifiers, specifically AS6, CO5, RE3, RE5, SD3, II5, and EI3 were identified as having a weak coefficient correlation fit. This indicates that while many of the items had a relatively high number of matching answers, the remaining answers between the two sets of data were widely spread across the answer scale. This can be interpreted as the item not being a reliable indicator or measure or that the question needs further refinement (MacKenzie et al., 2011; Petter et al., 2007). This viewpoint may have relevance to this study as the survey instrument provided an opportunity for participant feedback; and indicator identifier EB5 received numerous comments indicating that it was confusing and needed to be more clearly worded. Table 23 summarizes the test-retest results.

Table 23: Test-Retest Results

Observable Indicator Identifier	Associated Survey Question	Test-Retest Coefficient Correlation (Pearson's R)	Fit	Number & Percentage of Exact Test-Retest Answer Matches
AS1	A-1	0.438	acceptable	74 out of 91 (81.3%)
AS2	A-2	0.544	acceptable	66/91 (72.5)
AS3	A-3	0.488	acceptable	69/91 (75.8)
AS4	A-4	0.457	acceptable	70/91 (76.9)
AS5	A-5	0.605	strong	57/91 (62.6)
AS6	A-6	0.373	weak	59/91 (64.8)
AS7	A-7	0.413	acceptable	64/91 (70.3)
AS8	A-8	0.593	acceptable	63/91 (69.2)
CO1	B-1	0.450	acceptable	50/91 (54.9)
CO2	B-2	0.658	strong	67/91 (73.6)
CO3	B-3	0.530	acceptable	59/91 (64.8)
CO4	B-4	0.431	acceptable	65/91 (71.4)
CO5	B-5	0.274	weak	58/91 (63.7)
RE1	C-1	0.561	acceptable	55/91 (60.4)
RE2	C-2	0.507	acceptable	67/91 (73.6)
RE3	C-3	0.385	weak	60/91 (65.9)
RE4	C-4	0.561	acceptable	69/91 (75.8)
RE5	C-5	0.354	weak	57/91 (62.6)
SD1	D-1	0.618	strong	64/91 (70.3)
SD2	D-2	0.566	acceptable	63/91 (69.2)
SD3	D-3	0.310	weak	56/91 (61.5)
II1	E-1	0.431	acceptable	66/91 (72.5)
II2	E-2	0.419	acceptable	65/91 (71.4)
II3	E-3	0.512	acceptable	56/91 (61.5)
II4	E-4	0.503	acceptable	60/91 (65.9)
II5	E-5	0.275	weak	63/91 (69.2)
EI1	E-6	0.812	very strong	73/91 (80.2)
EI2	E-7	0.596	acceptable	66/91 (72.5)
EI3	E-8	0.299	weak	60/91 (65.9)
EI4	E-9	0.734	strong	74/91 (81.3)
EI5	E-10	0.660	strong	69/91 (75.8)
EI6	E-11	0.648	strong	73/91 (80.2)
EI7	E-12	0.655	strong	69/91 (75.8)
EB1	F-1	0.481	acceptable	60/91 (65.9)
EB2	F-2	0.734	strong	59/91 (64.8)
EB3	F-3	0.637	strong	52/91 (57.1)
EB4	F-4	0.418	acceptable	66/91 (72.5)
EB5	F-5	0.448	acceptable	49/91 (53.8)

For the reflective constructs Cronbach's alpha provides a measure of reliability. Table 24 displays the detailed results from the covariance based confirmatory factor analysis of the measurement model assessing indicator validity and reliability of the reflective constructs used in this study. As previously noted, the construct of External Influences is acceptable, while the constructs of Internal Influences and Ethical Behavior are acceptable as new items using the recommended value of 0.6 per Nunnally and Bernstein (1994) and minimally unacceptable by researchers using 0.7 as the accepted level.

Table 24: Reflective Constructs after Measurement Model Modification

Reflective Construct	Construct Identifier	Estimate	Standard Error	Standard Path	Z	Cronbach's alpha
Ethical Behavior						.592
	EB1	1.000		.606		
	EB2	1.199	.18	.489	6.64	
	EB3	.771	.13	.421	5.99	
	EB4	.980	.13	.647	7.44	
External Influences						.824
	EI1	1.000		.646		
	EI2	.864	.08	.672	11.10	
	EI3	.838	.09	.525	9.03	
	EI4	.891	.08	.632	10.57	
	EI5	.800	.07	.657	10.90	
	EI6	.693	.06	.677	11.17	
	EI7	.791	.07	.727	11.79	
Internal Influences						.633
	II2	1.000		.659		
	II4	1.030	.12	.577	8.28	
	II5	.937	.11	.590	8.39	

Multicollinearity

Indicator items under the same formative construct were also evaluated for potential multicollinearity. Conceptual overlap is indicated by an excessive degree of correlation between indicators, with high correlation being ≥ 0.90 and moderate being ≥ 0.80. All correlations between items under the same construct were found to be less than 0.6, providing evidence that there are no multicollinearity issues.

4.2.3 Structural Model Data Analysis Results

After establishing the appropriateness of the measurement model, an evaluation of the structural or inner model was performed. The structural equation modeling analysis for the TWEB structural model is presented in this section. Details regarding the specific indices chosen for reporting the analysis of the structural model are discussed in Section 3.5.4, Data Analysis. The primary emphasis of the inner model analysis was to establish the significance of the standardized path weights and *p*-values between the four ISS constructs of AS, CO, RE, and SD on Ethical Behavior, of Internal and External Influences on each of the ISS constructs and Ethical Behavior, and of External Influences on Internal Influences.

The variables of External Astuteness, External Conviction, External Rectitude, and External Self-Discipline represent the moderation effect of External Influences on the constructs of Astuteness, Conviction, Rectitude, and Self-Discipline respectively. The variables of Internal Astuteness, Internal Conviction, Internal Rectitude, and Internal Self-Discipline represent the moderation effect of Internal Influences on the constructs of

Astuteness, Conviction, Rectitude, and Self-Discipline respectively. A summary of the PLS inner model is presented in Table 25.

Model Fit

An examination of the standardized path weights of the four formative constructs revealed that Self-Discipline was the only ISS component with a statistically significant direct effect on Ethical Behavior, *Beta* = .131, *p* = .002; higher values for Self-Discipline were predictive of higher values for Ethical Behavior. This effect was also significantly moderated by Internal Influences, *Beta* = .257, *p* < .001; where at higher levels of the moderating construct, Self-Discipline made a stronger impact on Ethical Behavior.

Table 25: Summary of PLS Inner Model with Moderation Interactions

Variable	Path Weight	*SE*	*t*	*p*	R^2
Internal Influences					.280
External Influences	.529	.04	12.40	< .001	
Ethical behavior					.596
Astuteness	.052	.04	1.33	.185	
Conviction	.084	.04	2.20	.047	
Rectitude	.072	.04	2.10	.183	
Self-Discipline	.131	.04	3.20	.002	
External Influences	.048	.04	1.11	.267	
Internal Influences	.108	.04	2.52	.012	
External Astuteness	.005	.04	.120	.903	
External Conviction	.140	.05	2.70	.007	
External Rectitude	-.403	.05	7.53	< .001	
External Self-Discipline	-.106	.05	1.96	.051	
Internal Astuteness	.575	.04	12.90	< .001	
Internal Conviction	-.002	.05	.040	.964	
Internal Rectitude	.382	.05	7.83	< .001	
Internal Self-discipline	.257	.05	4.69	< .001	

The path weights of the formative constructs of Astuteness, *Beta* = .052, *p* = .185; Conviction, *Beta* = .084, *p* = .047; and Rectitude, *Beta* = .072, *p* = .183; did indicate a positive effect, albeit small. The Internal Influences construct also significantly moderated the effects of Astuteness and Rectitude, *Beta* = .575, *p* < .001 and *Beta* = .382, *p* < .001. In both cases, higher levels of Internal Influences gave rise to a positive relationship between the formative constructs and Ethical Behavior, while lower levels of Internal Influences created the opposite effect. The effect of Internal Influences on Conviction, were insignificant, *Beta* = -.002, *p* = .964. Figure 11 depicts the effects of the moderator Internal Influences on the relationships between the four ISS components and Ethical Behavior.

Higher levels of the External Influences construct had a positive, but not very strong, moderating effect between Astuteness, *Beta* = .005, *p* = .903; Conviction, *Beta* = .140, *p* = .007, and Ethical Behavior respectively. Higher levels of External Influences had a slight negative moderation effect between Self-Discipline, *Beta* = -.106, *p* < .051, and Ethical Behavior. In the case of Rectitude, *Beta* = -.403, *p* < .001, a positive effect on Ethical Behavior was observed at lower levels of External Influences, while an opposite effect was observed at higher levels of External Influences. Figure 12 displays the moderation effect of External Influences on the relationships between the four ISS components and Ethical Behavior.

The reflective construct of External Influences explains just under 30% of the variation (R^2 = .280) in Internal Influences, where higher values of External Influences on the construct of Internal Influences corresponded with higher values of External Influences, *Beta* = .529, *p* < .001. As Internal and External Influences were conceptualized as separate entities, 30% appears to be acceptable as it is not expected that the R-squared value would show predictive power of one construct over the other by being too high. The 30% variance provided evidence that External Influences affects Internal Influences, and also confirms the distinction of the two.

The TWEB model, which consists of the four virtue ethics constructs, the influencers, and the interactions between all constructs; explained almost 60% of the variation ($R^2 = .596$) in the dependent variable Ethical Behavior which is considered a fairly high R-squared in behavioral sciences and is considered a good fit.

A graphical representation of the structural model detailing the TWEB model construct connections is presented in Figure 13. Thicker lines denote the statistically significant path weights at $\alpha = .05$.

Figure 11: Moderation Effect of Internal Influences

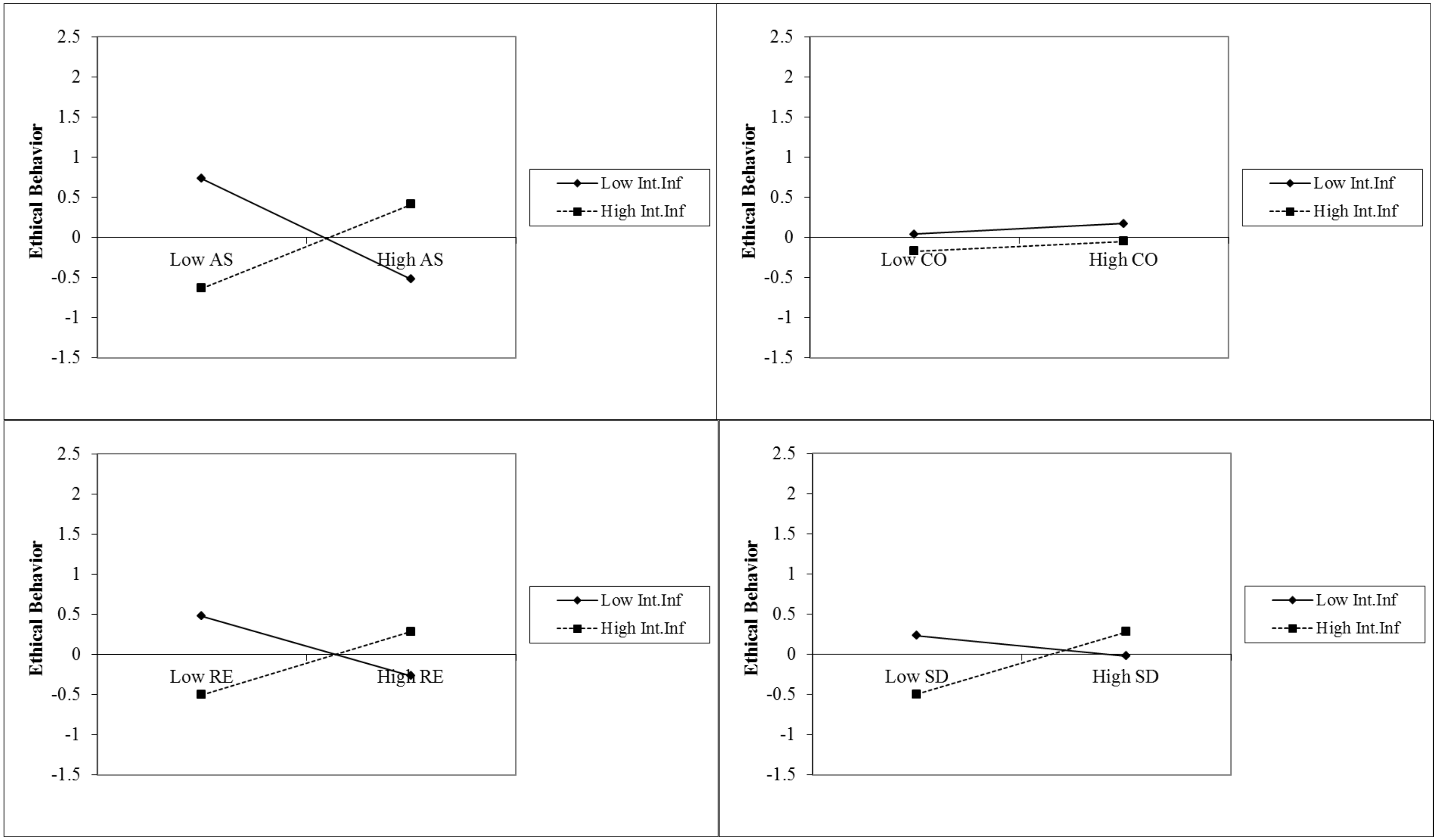


Figure 12: Moderation Effect of External Influences

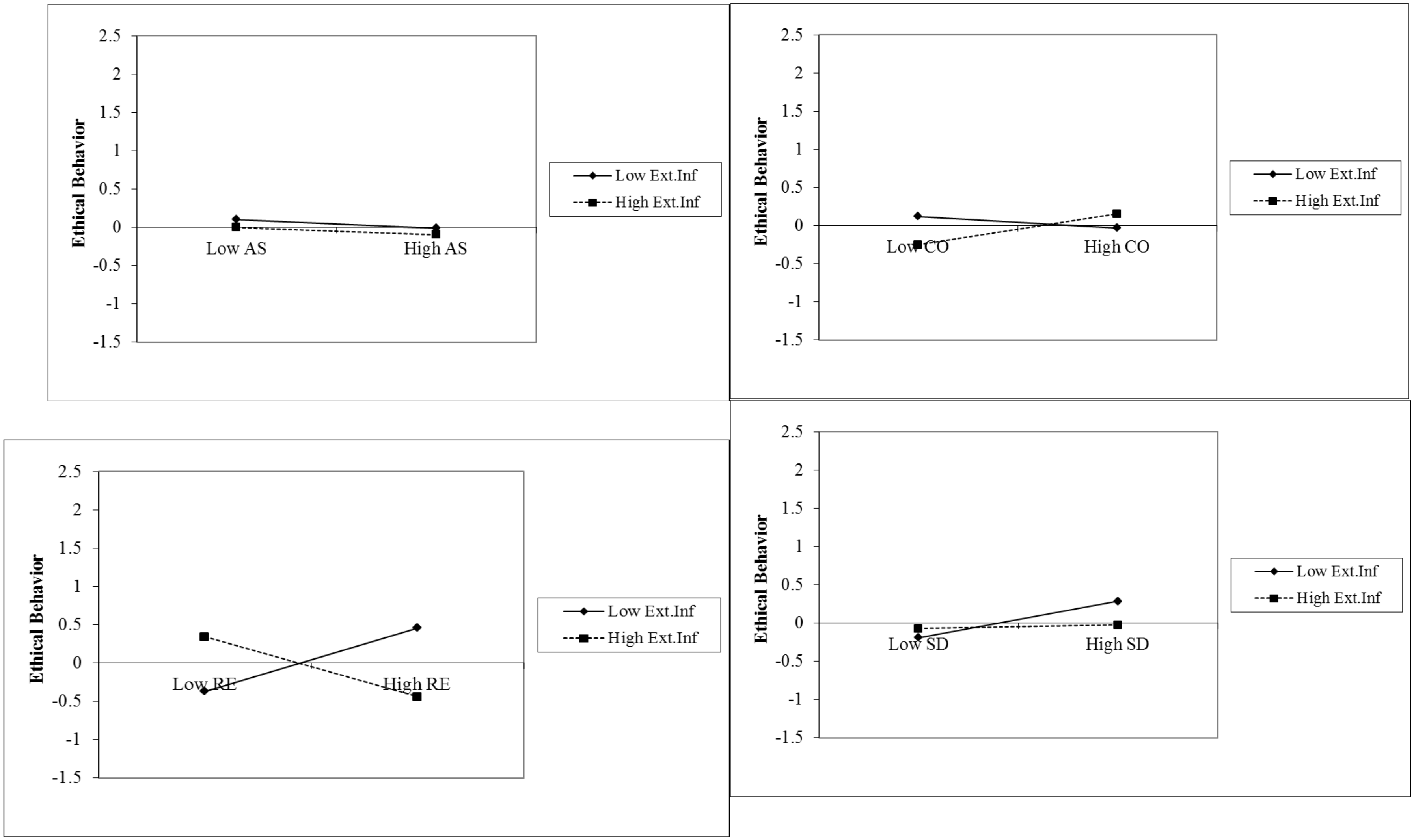
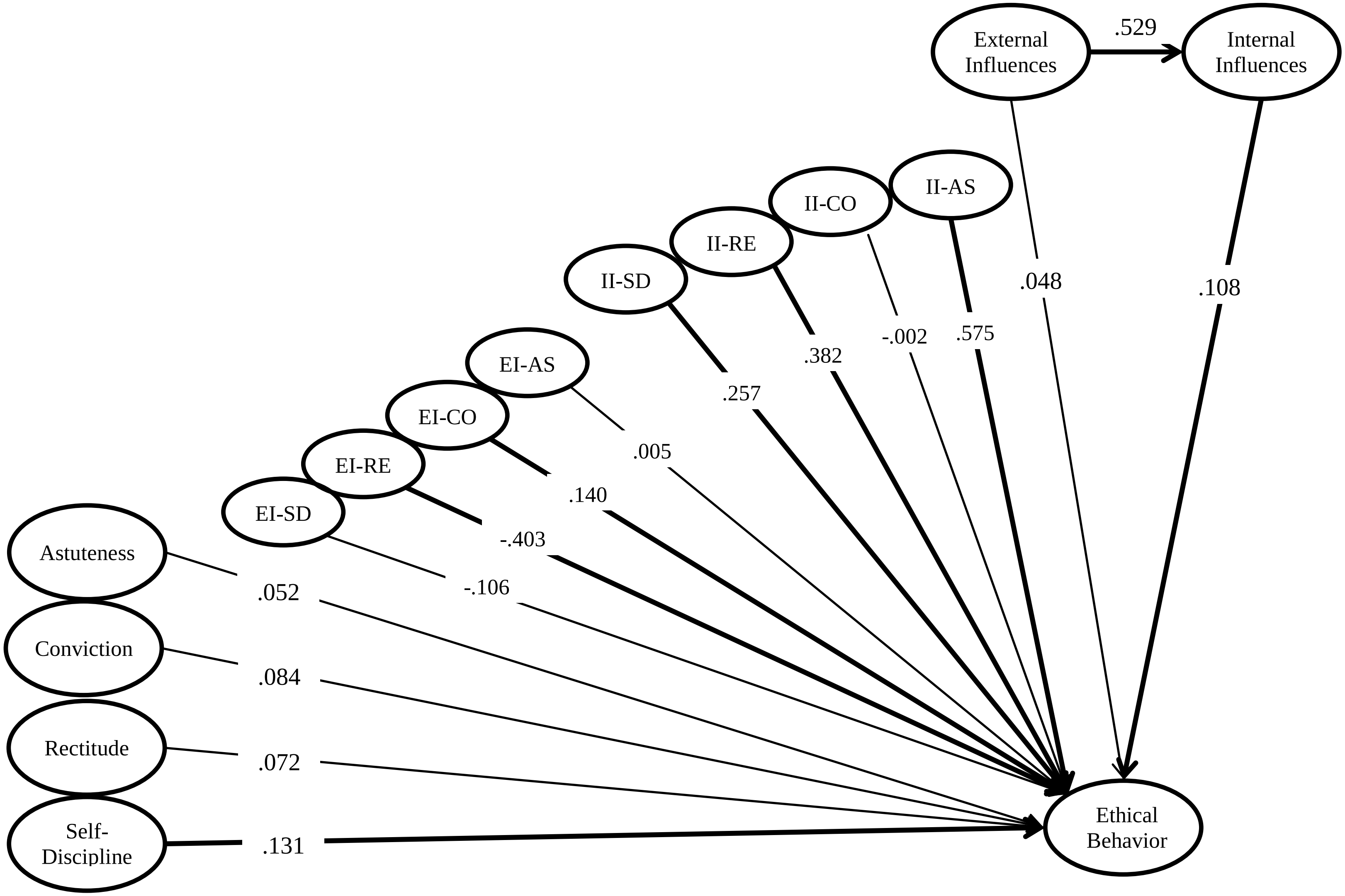


Figure 13: Inner PLS Model Displaying Structural Relations



Hypotheses Testing

A PLS model was fitted to the data to test the seven hypotheses presented in this study. Specific details regarding the hypotheses are in Chapter 3.4, Research Hypotheses. The hypotheses, the relationships between constructs, and results are presented in Table 26.

Table 26: Hypothesis Relationship Results

Hypothesis	Link	Relationship	*p*-value	Result
H1	AS → EB	positive	.185	not significant
H2	CO → EB	positive	.047	significant
H3	RE → EB	positive	.183	not significant
H4	SD → EB	positive	.002	significant
H5	EI → AS	positive	.903	not significant
H5	EI → CO	positive	.007	significant
H5	EI → RE	negative	<.001	significant
H5	EI → SD	negative	.051	significant
H6	II → AS	positive	<.001	significant
H6	II → CO	negative	.964	not significant
H6	II → RE	positive	<.001	significant
H6	II → SD	positive	<.001	significant
H7	EI → II	positive	<.001	significant

While not all *p*-values were significant, when there are interactions in a model such as the moderators of Internal and External Influences, the significance of a single path coefficient cannot be relied upon to determine if a particular hypothesis holds. In these cases, the results must be evaluated more closely (Kutner, Nachtsheim, Neter, & Li, 2005). Positive relationships are typically interpreted as being synonymous with good or acceptable; however, positive relationships between variables can be decreased because of negative influences.

Additionally, it has been noted by Hair et al. (2009) that *p*-values associated with weights and loadings are subject to the related survey items being misunderstood by the survey participants as the researcher intended. Several questions in this research study's survey were noted as unclear by participants, which may have affected the significance of the associated *p*-value.

4.3 Findings

Several goodness of fit tests were performed on the reflective portion of the measurement model and the fit was evaluated as good, with the indices of χ^2/df, RMSEA, SRMR, and CFI being acceptable. NNFI was determined to be marginally unacceptable. There are no applicable goodness of fit tests for the formative portions of the outer model.

Convergent validity was evaluated as acceptable for the reflective constructs of External Influences and Internal Influences. The construct of Ethical Behavior was marginally less than acceptable. Convergent validity results are not applicable to the outer model's formative constructs.

Discriminant validity for the reflective constructs was evaluated by comparing AVE correlations between latent variables and all were found to be acceptable. Formative construct discriminant validity was evaluated using indicator path weights and loadings. Four indicator items, specifically AS3, AS4, AS5, and RE2, were found not to be significant predictors of their associated construct; however, based on cited research they were retained in the model. All other formative construct indicator were found to be significant predictors of their construct.

Data distribution normality was evaluated using kurtosis and skew and was found to be within acceptable norms.

Reflective construct reliability was evaluated using Cronbach's alpha and based on their standardized weights were found to be acceptable. Using non-standardized weights the construct of Ethical Behavior was identified as marginally unacceptable. Formative construct reliability was evaluated using inter-rater agreement and test-retest. Inter-rater agreement assessment found that the majority of reflective indicator items had acceptable reliability; only one item significantly exceeded one standard deviation (SD). Inter-rater agreement for all formative constructs were determined to have acceptable reliability; although four indicator items slightly exceeded one SD. Test-retest was also used to assess formative construct reliability with 16 of 21 indicators demonstrating acceptable reliability. Only one indicator item, RE5, demonstrated weak reliability on both assessment scales.

Construct indicator items were evaluated for conceptual overlap and no multicollinearity issues were found.

The evaluation of the structural model's validity and interactions indicated that the relationship between the constructs of Self-Discipline and Ethical Behavior had a significant path weight, and the constructs of Astuteness, Conviction, and Rectitude had less significant but positive effect on Ethical Behavior. The effects of External Influences and Internal Influences on Ethical Behavior were positive, with Internal Influences being most significant. An evaluation of the moderating effects reveals that External Influences had a significant moderating effect on Conviction, Rectitude, and Self-Discipline; however, its effect on Astuteness was negligible. Internal Influences had a significant moderating effect on Astuteness, Rectitude, and Self-Discipline; however, its effect on Conviction was negligible.

The effect of External Influences on Internal Influences was significant, explaining almost 30% of the variance. The various interactions between all components of the TWEB model explain almost 60% of the variance on the Ethical Behavior dependent variable.

As noted in Chapter 3, not all indices used in model evaluation will meet acceptable values and a model should not be considered invalid because of the shortcomings of a particular index. In regards to the measurement model, it must be noted that measurements conducted for this study were not as reliable as hoped. Goodness of fit results were mixed. Low reliability and convergent validity for reflective constructs, and insignificant paths from items to formative constructs suggest that more care is necessary in measuring the constructs. Low loadings may be a result of inappropriate items, poorly worded survey items, or the improper transfer of the item from one context to another. Hooper et al. (2008) point out that a strict adherence to cutoff values can lead to the rejection of an acceptable model. Further evaluation of the data collection process should point to possible improvements for future research.

Hypothesized relationships of the TWEB model were examined based on *p*-values. Hypotheses H2, H4, and H7 were fully supported. Hypotheses H5 and H6 were each comprised of four components. In each hypothesis, three of the components were fully supported; the remaining component in each demonstrated an effect, albeit not statistically significant. Nonetheless, H5 and H6 were each considered supported. H1 and H3 each demonstrated a positive relationship through path weights; however, the weights were small and not statistically significant. Prior research has shown that when there are interaction items such as mediators or moderators in a model, researchers cannot rely on a single path coefficient to determine if a hypothesis is valid. A closer evaluation of the interaction effects must be performed (Chin, 2010). Additionally, tests of significance often incorrectly lead to the rejection of a hypothesis; and that small but significant results can be obtained with large sample sizes (Coe, 2002; Hooper et al., 2008; Kline, 1998). Because the path weights in this study were based on a large sample the hypotheses of H1 and H3 were considered partially supported.

4.4 Summary of Results

The IA and ISS SME survey participants provided data in which to empirically evaluate the TWEB outer model using CB-SEM for the reflective constructs and PLS-SEM for the formative constructs. PLS-SEM was also used to evaluate the inner model. The TWEB measurement model evaluation focused on the validity and reliability of the indicators that represented the constructs and provided an assessment of their goodness of fit, data set normality, convergent and discriminant validity, reliability, crossloading issues, and multicollinearity.

The various tests determined the validity and reliability of the measurement model, and while some of which were not as strong as preferred, they were adequate and provided the basis on which to establish the validity of the results of the structural model evaluation.

The validity of the formative constructs, the relationships between the seven constructs of the structural model, as well as the seven proposed hypotheses were evaluated through the significance of their path weights and *p*-values. All of the relationships between constructs were positive, although some were stronger and more significant.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

5.1 Introduction

Research shows that trusted workers, individuals who possess elevated privileges on an information system (IS), are seen as a significant threat to the systems security. The primary purpose of this research was to propose a means of addressing insider threats to information systems by identifying the factors which affect and influence trusted worker ethical behavior. A better understanding of these factors has the potential to be used by organizations to influence trusted worker ethical commitment and intentions. Virtue ethics based concepts were advanced as a means to potentially align and influence the moral values and behaviors of information system security (ISS) trusted workers with those of their employing organization in order to better protect IS assets.

Four new virtue ethics based individual morality ISS constructs were proposed, potential indicators identified, and it was suggested how they may influence the character development and moral choices of information system security workers. A trusted worker ethical behavior model was advanced which provided a framework in which to recognize these internal motivations and determine if it is feasible and effective to incorporate, either individually or collectively, the four proposed ISS constructs into the various internal processes of an organization in order to positively shape, guide, or influence the ethical evaluations, actions, and behavior of IS trusted workers. Potential indicator items for each of the constructs were identified through a literature and expert panel review, and after refinement and checks for content validity, the final list consisted of 38 statements. The theoretical model's constructs and indicators were empirically tested through confirmatory factor analysis and structural equation modeling using data collected from the responses of 395 survey participants.

This chapter presents the research conclusions, implications, and contributions to the information system security community; limitations, recommendations, and opportunities for future research; and a summarization of the study and its findings.

5.2 Conclusions

The goal of this study was to determine the applicability of the cardinal virtues and to identify key elements of virtue ethics which may be applicable to ISS in order to better understand those individuals who may be an insider threat to an information system. The results of this research provides empirical evidence that a virtue ethics based ISS methodology can positively affect ethical behavior. Seven hypotheses were tested, and the following were supported:

H2: *Increased ISS Conviction will have a positive effect on trusted worker ethical behavior.*

H4: *Increased ISS Self-Discipline will have a positive effect on trusted worker ethical behavior.*

H5: *Organizational internal influences moderate the effect of the four virtue ethics constructs on trusted worker ethical behavior.*

H6: *External influences on trusted workers moderate the effect of the four virtue ethics constructs on trusted workers.*

H7: *External influences on trusted workers affect how organizational internal influences are interpreted.*

The path weights of the following hypotheses, although positive, were considered small, and their *p*-values were not statistically significant:

H1: Increased ISS Astuteness will have a positive effect on trusted worker ethical behavior.

H3: Increased ISS Rectitude will have a positive effect on trusted worker ethical behavior.

An important question regarding results is not how big the results are, but rather are they big enough to mean something. In studies with large samples, Kline (1998) cautions that relying solely on the results of tests of significance often incorrectly leads to the rejection of a hypothesis. This approach to hypothesis testing is also recommended by Kutner, Nachtsheim, Neter, and Li (2005); it is emphasized that researchers should look beyond just an effect magnitude or *p*-value, and make informed conclusions about the results they have obtained. An arbitrary fit value may hinder thinking about what results really mean (Ellis, 2010). Chin (2010) elaborates further, stating that a lack of model goodness of fit does not mean necessarily mean lack of a good model. Therefore, hypotheses *H1* and *H3* are not rejected outright, but it is recommended that they, as well as the rest of the TWEB model, undergo further refinement and study. The current conclusion by this researcher is that it is a good model with some non-significant components. All four virtue ethics based constructs are making an impact on ethical behavior, and the effects are moderated in one way or another by internal and external influences. Additionally, external influences significantly affect internal influences.

The results of this research provide insight for understanding the components and influences on the intentions and behavior of ISS trusted workers. As noted by Warkentin and Willison (2009) approaches to addressing the problem of insider threats should consider methodologies learned from other behavioral sciences such as ethics. The practice of virtue ethics and the resulting ethical construction or shaping of a moral agent inevitably influences the ethical makeup of the organization the subject interacts in (Floridi, 2010). According to Bright et al., (2014), the properties that make up organizational virtue need to be explored. An understanding of virtue is important and essential for organizational ethics; however, virtues - while often promoted - are seldom practiced.

The findings of this study suggest that an employee’s ethical behavior intentions are formed in part by the direct effects of the four ISS virtues, and indirectly from influences external and internal to the organization. The findings also imply that employee security compliance intentions can potentially be identified through a personnel screening process or background investigation that interprets their approach to ethical challenges. These intentions and approaches may be shaped by external influences in an employee’s personal life; and further shaped through influences internal to their employing organization such as organized training programs with focused, repetitive learning and instruction activities based on virtue ethics based ISS principles. Developing an interview instrument which can identify virtue ethics related aspects of a potential new hire’s background might provide insight as to whether the individual is ethically and morally well-grounded and therefore a good fit for the hiring organization, particularly into positions that grant elevated privileges or access to business sensitive information, trade secrets, or intellectual property. Using processes developed from this methodology to identify a trusted worker's style of ethical decision making and to develop more ethical employees may result in a more ethical organizational environment, thereby reducing the possibility of insider threats.

5.3 Implications

The implications of this study are that it provides researchers with the evidence that virtue ethics has potential application in the field of ISS, assuming that any concerns that practitioners may have can be addressed. It also provides practitioners with alternatives to technical controls, checklists, and formal procedures; which are accepted as being generally ineffective against determined insiders. This research also establishes practitioner consensus on the indicators of new, formative virtue ethics based ISS constructs that can be explored, expanded upon, and validated by both the researcher and practitioner communities. After undergoing validation and reliability testing in this study, these constructs can now potentially be operationalized to predict a worker's future ethical behavior thereby improving ISS.

Practitioner Implications

This research supports the contention that an increased emphasis on the hiring, training, motivational, and behavioral processes based in virtue ethics methodologies could be of benefit to organizational information system security; and that a virtue ethics based approach to ISS has the potential to be effective. Results can be used to develop processes, instruments, and tools to assess the ethical commitment of employees.

Employee pre-hire screening and periodic assessments of current employees may be a means of identifying the types of external influences on an individual's behavior. Identifying employees and potential new hires who have been exposed to external influences based in virtue ethics may be of benefit by ensuring that the moral or ethical foundation of those personnel is aligned with the expectations of the organization. It is recommended that some level of detail regarding these influences be solicited from the subject individual so that associations can be assigned to what the organization considers to be positive virtue ethics influences.

Organizations desiring to improve compliance with information system security requirements should consider implementing a virtue ethics based approach to training employees about decision making related to ISS. Employees could be assigned to a mentor and participate in virtue ethics focused on-the-job training which facilitates the continuous inculcation of virtuous practices in order to promote acquisition and development of desired decision making habits.

Researcher Implications

This study provides a starting point for further research into virtue ethics based concepts for addressing behavioral issues related to maintaining ISS. It conceptualizes the interactions of the components and indicators of a trusted worker ethical behavior model and provides a framework for future research.

Additionally, understanding the benefits of a virtue ethics based approach to ISS provides insight into addressing the issue of insider threats, specifically in regards to the influences and motivators of those individuals who possess elevated privileges on an information system.

5.4 Limitations

Five limitations of this study’s results were identified. The first is generalization. While the demographic information was self-reported; the characteristics and range of professional roles, education, experience, expertise, and certifications of this study’s participants are considered to be an accurate representation of the population they are intended to represent. However, the target population for this study was members of only one professional organization, albeit one of international scope with a large member base. While a large enough sample might be generalizable, the findings are specific to that organization. It is a possibility that the data gathered in this study is not representative of other security organizations or professionals. Further studies should be conducted with users from other institutions to more confidently generalize the findings.

The second limitation rests with the fact that the invitations to participate in the study were sent via e-mail. This raises the possibility that users may not have received the invitations; or that they were ignored, forgotten, or identified as spam, thereby lowering the response rate. Coverage error, when the sample does not represent all the characteristics of the population, is another possible issue as the demographic data being gathered relies on self-reporting by the individual respondents. This was mitigated by only distributing survey invitations to members of an organization which is comprised of information system security professionals, therefore their credentials have already been vetted to some degree by that organization.

Third, the background of the participants was that of practitioners, they may not have had the benefit of being familiar with the relevant research literature on the subject of virtue ethics. Also, the predominate mindset of the participants for addressing ISS issues was likely through the use of technical controls, which may have affected their consideration or acceptance of ethical concepts and solutions.

Fourth, participation from certain participants such as IA/IS students and specialists may be under or over represented. This could have skewed the results in a particular direction based on the viewpoint of the participants and not accurately represent the opinions of the ISS community as a whole.

The fifth limitation is that while the trusted worker ethical behavior or TWEB model is generally good fitting and appears to demonstrate the relationships and factors which influence the ethical commitment of information system workers placed in trusted positions, it is plausible that other iterations of the model that were not tested may produce better levels of fit. However, any modifications to the model should be warranted theoretically rather than based on data analysis results which suggest the addition or deletion of particular parameter that may be statistically insignificant. As noted by Schreiber et al. (2006) and Jackson et al. (2009), use of alternate models or making arbitrary changes to a model to improve fit increases the possibility of a Type 1 error.

All of these limitations may affect the validity of the results.

5.5 Recommendations for Future Research

This study can be viewed a springboard for additional research. As noted by MacKenzie et al. (2007), construct and measurement development and validation is an ongoing process. Future research should be conducted in order to provide further evidence in which to verify the validity of this study and extend the results.

The demographic information requested of survey participants did not include age or gender data. Age and gender attitudes towards ethical concepts and issues may affect survey results or provide different insights. Future surveys could focus on obtaining results from specific professional roles, for example those of individuals filling executive positions, to determine any differences in their ethical deliberations. Additionally, expanding the study to other organizations – particularly to other international organizations, may be of interest. In the latter's case, consideration must be taken when designing the survey instrument as other cultures may have different interpretations of ethical behavior. There is also the issue of having an accurate translation of the survey instrument in order to prevent any loss or change of the researcher's intent or meaning.

Many researchers (Diamantopoulos, 2011; Jarvis et al., 2003; MacKenzie et al., 2011; Petter et al., 2007) recommend having formative constructs identified through two paths of either measurement relations, structural relations, or a mixture of both in order to support covariance based SEM. Future research could focus on the effect of adding another second order construct with reflective indicators such as "Organizational IS Security Success" to the TWEB model as a method of eliminating any question of formative construct misidentification as recommended by Diamantopoulos (2011).

Alternately, two distinct reflective indicators that capture its intent could be assigned to each formative construct.

The TWEB model construct indicator items should be further developed and refined using the MacKenzie et al. (2011) Scale Development Procedure. The survey instrument can then be improved based on those refinements. Additionally, statistical analysis could be conducted on the existing or new survey data using a software program that can calculate R^2 on formative constructs as this was a shortcoming in this study. The ability to accomplish this particular statistical analysis procedure would allow the determination of the variance of the formative portion of the TWEB model, which is one of the recommended measures of structural model validity in PLS.

Future research could also evaluate if ISS workers who have been identified as having been exposed to virtue ethics based principles outside of their work environment or who have received ongoing organizational training centered on virtue ethics concepts do in fact demonstrate increased security compliance or improved on-the-job ethical behavior.

5.6 Summary

The failure of the practitioner community to address insider threats, particularly in regards to the ethical failures of trusted workers, including senior management and employees with privileged access who can affect an information systems security posture, demand that innovative solutions beyond technical controls, checklists, and formal procedures be explored. This study has built upon the work of Weber (1981, 1993) and Floridi (1999, 2006) to develop a model for ISS trusted worker ethical behavior based on new, formative constructs. The effect of these constructs results in reflected behavior that affects trusted worker ethical behavior, and ultimately the ISS within an info-sphere such as a business organization.

The objective of this study was to confirm through statistical analysis the applicability of four virtue ethics based constructs as they relate to information system security by validating each construct's indicators and factors which influence the ethical commitment of information system workers placed in trusted positions. This was done through an examination of those components and their relationships in an ethical behavior model. The focus of the study was the TWEB model; which consists of four virtue ethics ISS constructs, two influencer constructs, and one ethical behavior construct. The research methodology used was the survey method, utilizing an anonymous web-hosted questionnaire. The survey population consisted of SMEs from an international ISS professional organization based in the USA. Confirmatory factor analysis was used to determine causal patterns in the variables and assess them for validity and reliability in the proposed theoretical model. Structural equation modeling was then used to test for casual relations between the model's constructs.

The findings of this study regarding virtue ethics as they are applicable to ISS present a solid initial understanding of the concepts and provide a foundation on which to guide further research and analysis of the related construct structural model, the Information System Security Trusted Worker Ethical Behavior Model. This conceptual model serves as the basis for a virtue ethics based approach to addressing insider threats to information systems security.

The TWEB model can serve as a powerful conceptual tool to illustrate the relationships between various key elements that affect the ethical behavior of ISS trusted workers. The model extends Floridi’s Information Ethics Model by incorporating internal and external influences into an info-sphere which may shape a moral agent’s ethical deliberations. The TWEB model is useful in promoting conceptual shifts in approaches to information systems security by engendering a virtue ethics based viewpoint. Practitioners may use the model to develop a comprehensive awareness of the impact that virtue ethics may have on employee behavior; develop employee ethics education and training programs, standards of conduct, and guidelines for ethical responsibilities and behavior; and to incorporate pre-employment screening processes and tools which identify the approach or style that an potential employee make take to ethical decision making. The ethical decision making approach that is identified may be one that the organization finds preferable or not in its employees. Researchers can use the model to reflect on the applicability of the virtues to ISS and to further explore their interactions and influences on trusted worker behavior.

The ultimate goal of incorporating an ethics approach based on the TWEB model is for ISS professionals to practice more ethical behavior. Not because of organizational policies and procedures, rewards and punishment, or managerial oversight or peer pressure; but rather as a result of their own internal motivations. Based on the results of this research, a virtue ethics based methodology that induces employees to make ethical decisions that were internalized as “the right thing to do” both as a professional and for the organization appears to be an effective approach to reducing insider threats to information systems.

Appendix A

Acronyms

AMOS	Analysis of Moment Structures
AVE	Average Variance Extracted
CB-SEM	Covariance Based Structural Equation Modeling
CEO	Chief Executive Officer
CFA	Confirmatory Factor Analysis
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity, and Availability
CFI	Comparative Fit Index
CISSP	Certified Information Systems Security Professional
DOD	Department of Defense
FBI	Federal Bureau of Investigation
GDT	General Deterrence Theory
IA	Information Assurance
IAWF	Information Assurance Workforce
ICT	Information Computing Technology
IE	Information Ethics
IEC	International Electrotechnical Commission
IRB	Institutional Review Board
IS	Information System
ISO	International Organization Standardization
ISS	Information Systems Security
IT	Information Technology
LISREL	Linear Structural Relations
NNFI	Non-Normed Fit Index
NSA	National Security Agency
PLS	Partial Least Squares
PLS-SEM	Partial Least Squares Structural Equation Modeling
RMR	Root Mean Square Residual
RMSEA	Root Mean Square Error of Approximation
RPT	Resource Product Target
SD	Standard Deviation
SEM	Structural Equation Modeling
SME	Subject Matter Expert
SRMR	Standardized Root Mean Square Residual
SSPS	Statistical Product and Service Solutions
TWEB	Trusted Worker Ethical Behavior
US	United States

Appendix B

Research Model Variables and Indicators

Research Model Variable	Observable Indicator Identifier	Description of Observed Indicator	Associated Survey Question
ISS Astuteness	AS1	Making morally right decisions is a part of ethical computer behavior	A-1
	AS2	Impartial decision making by workers can influence their information system security compliance	A-2
	AS3	An ability to make decisions based on professional experience contributes to information system security	A-3
	AS4	User awareness of the appropriate and correct use of an information system can affect the systems security	A-4
	AS5	Consistent behavior is necessary when an employee performs security actions on an information system	A-5
	AS6	An individual’s ability to resolve conflicts between organizational policies and goals can impact the security of an information system	A-6
	AS7	Being able to recognize ethical issues has an effect on information system security	A-7
	AS8	Information system security is affected by an employee’s technical skills	A-8
ISS Conviction	CO1	Computer ethics involves making self-determinations rather than making choices expected by others	B-1
	CO2	Computer ethics involves how an individual should act in particular situations	B-2
	CO3	A focus on the greater good over personal desires promotes good computer ethics	B-3
	CO4	Making correct judgments contributes to information system security policy compliance.	B-4
	CO5	Regarding information system security, when an individual commits an unethical act they will try to rationalize to themselves that their behavior is acceptable	B-5
ISS Rectitude	RE1	Civic responsibility and civic participation are elements of ethical computer behavior	C-1
	RE2	There is a relationship between ethical computer behavior and safeguarding sensitive information	C-2
	RE3	Ethical computer behavior involves making decisions that may affect society	C-3

Research Model Variable	Observable Indicator Identifier	Description of Observed Indicator	Associated Survey Question
ISS Rectitude	RE4	Ethical use of an information system is important to an organization whether or not business goals are achieved	C-4
	RE5	Being sensitive to loss of information system data is an ethics related issue	C-5
ISS Self-Discipline	SD1	Information system security compliance is affected by a person's attitudes and beliefs	D-1
	SD2	Employee professionalism promotes information systems security	D-2
	SD3	Employees enhance information system security compliance by making rational decisions	D-3
Internal Influences	II1	Ethical guidance provided to employees by an organization is an effective method of achieving desired behavior	E-1
	II2	The actions of senior managers influence whether employees conform to expected organizational policies or rules	E-2
	II3	Rewards and punishment are effective incentives for achieving compliance with organizational expectations	E-3
	II4	Cost, schedule, and performance requirements affect employee compliance with business requirements	E-4
	II5	The morale level (esprit de corps) of an organization plays a role in employee behavior	E-5
External Influences	EI1	An individual's actions may be dictated by their religious beliefs	E-6
	EI2	A person's opinion of what is acceptable behavior is determined by their cultural background	E-7
	EI3	Personal factors or variables such as age, gender, and life experiences contribute to an individual's concept of "right" behavior	E-8
	EI4	An individual's ethical foundation is affected by their participation in social organizations	E-9
	EI5	Friends and peers impact a person's sense of right and wrong behavior	E-10
	EI6	Events in an employee's personal life can affect their behavior at work	E-11
	EI7	An employee's personal beliefs play a role in how they react to an organizations behavioral guidelines	E-12

Research Model Variable	Observable Indicator Identifier	Description of Observed Indicator	Associated Survey Question
Ethical Behavior	EB1	Employees follow organizational policies and rules when making decisions regarding information system security	F-1
	EB2	In the absence of specific organizational guidance employees do not deviate from information system security best practices	F-2
	EB3	An organization experiencing a reduction in the number of events involving loss or compromise of information is an indicator of employee ethical behavior.	F-3
	EB4	Employees exhibit concern with the well-being of the organization by protecting organizational information and information technology assets	F-4
	EB5	An example of ethical behavior is when employees feel comfortable in disclosing security issues even if they believe other employees or the organization may disagree with them.	F-5

Appendix C

Survey Instrument

Information Systems Security Trusted Worker Ethical Behavior and Influences Survey

The purpose of this questionnaire is to solicit your input on the key elements of virtue ethics based information systems security (ISS) constructs for information systems (IS) trusted workers; defined as individuals who hold elevated access privileges or that can make decisions that affect the security posture or configuration of an IS. Completing and submitting the survey indicates your voluntary participation in the study. Survey participants will remain anonymous to each other and all survey answers will remain confidential. The survey consists of 44 questions.

Virtues are lasting character traits that can be learned through training and repeated practice. Once learned they are manifested in a person's behavior and become associated with their personality. These virtue ethics based constructs consist of the desired ethical characteristics of IS trusted workers that if exercised, or not, effect the security of an IS. The proposed constructs are:

Security Astuteness

Security Rectitude

Security Conviction

Security Self-Discipline

A review of applicable literature has initially identified potential construct elements, influences on employee ethical choices, and indicators of ethical behavior as reflected in Section Two of this survey. You will be asked to select a level of agreement that represents your attitude toward various items.

Section One:

The following questions are intended to collect basic demographic information and professional characteristics of participants so we can better understand the results of this survey.

1. Are you currently employed directly in the information system security field?

   Yes _____

   No ______

2. Which of the following job titles or categories best describes your current professional role?

   _____ Executive {Chief Executive Officer (CEO), Chief Information Officer (CIO), Chief Technology Officer (CTO), Information Technology (IT) Director, Deputy CIO, et cetera}

   _____ Information Assurance Manager (IAM) or Information Assurance Officer (IAO)

   _____ IT Department Head, IT Division Head, or IT Manager

   _____ Information Assurance or Information Security Specialist

   _____ IT Specialist

   _____ Information Assurance, Information Systems, or IT Student

_____ Other (please specify) _______________

3. What is the highest level of education you have completed?

Some High School _____

High School Diploma _____

Some College _____

Associate Degree _____

Bachelor’s Degree _____

Advanced Degree _____

Other _____

4. If you have obtained a college degree, is the major in the information assurance, information systems, information technology, or information computing technology field?

Yes _____

No _____

Not applicable _____

5. How many years of information system security experience do you have?
(Round up or down as necessary)

0-5 _____

6-10 _____

11-15 _____

16 or greater _____

6. Do you hold a professional certification in information system security such as Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), CompTIA Security+, or SANS Global Information Assurance Certification (GIAC)?

Yes _____

No _____

Section Two:

In this part we are seeking your opinions about the potential behaviors, behavioral influences, and their implications on information system security workers. After each question a five point scale is provided. Please indicate your level of agreement with the statements using the scale. You are encouraged to reflect upon your past experience when responding.

Scale:

1 = Strongly Disagree

2 = Disagree

3 = Neutral

4 = Agree

5 = Strongly Agree

If you desire to provide additional input or feedback there will be an opportunity at the end of the survey.

A. The following is a list of items related to Security Astuteness, which is defined as "skill in making assessments and in the application of professional knowledge, experience, understanding, common sense, or insight in regards to information system security."

Please indicate your level of agreement that the following items or statements are applicable elements of Security Astuteness:

1. Making morally right decisions is a part of ethical computer behavior.

SD	D	N	A	SA
1	2	3	4	5

2. Impartial decision making by workers can influence their information system security compliance.
3. An ability to make decisions based on professional experience contributes to information system security.
4. User awareness of the appropriate use of an information system can affect the systems security.
5. Consistent behavior is necessary when an employee performs security actions on an information system.
6. An individual’s ability to resolve conflicts between organizational policies and goals can impact the security of an information system.
7. Being able to recognize ethical issues has no effect on information system security. (R)
8. Information system security is affected by an employee’s technical skills.

B. The following items are related to Security Conviction, which is defined as “fixed or firmly held beliefs regarding information systems security that affect decisions regarding compliance.”

Please indicate your level of agreement that the following statements are applicable elements of Security Conviction:

1. Computer ethics involves making self-determinations rather than making choices expected by others.
2. Computer ethics involves how an individual should act in particular situations.
3. A focus on one's personal desires over the greater good is an example of good computer ethics. (R)
4. Making correct judgments contributes to information system security policy compliance.
5. Regarding information system security, when an individual commits an unethical act they will try to rationalize to themselves that their behavior is acceptable.

C. The following items are related to Security Rectitude, which is defined as "rightness or correctness of conduct and judgments that could affect information system security."

Please indicate your level of agreement that the following items or statements are applicable elements of Security Rectitude:

1. Civic responsibility and civic participation are not elements of ethical computer behavior. (R)

2. There is no relationship between ethical computer behavior and safeguarding sensitive information. (R)

3. Ethical computer behavior involves making decisions that may affect society.

4. Ethical use of an information system by employees is not important to an organization as long as business goals are achieved. (R)

5. Being sensitive to loss of information system data is a computer ethics related issue.

D. The following items are related to Security Self-Discipline, which is defined as "willpower and control over one's personal desires and conduct when considering actions that affect information system security."

Please indicate your level of agreement that the following items are applicable elements of Security Self-Discipline:

1. Information system security compliance is not affected by a person's attitudes and beliefs. (R)

2. Employee professionalism promotes information systems security.

3. Employees enhance information system security compliance by making rational decisions.

E. The following is a list of items relating to factors which may exert influence on the ethical makeup, choices, or behavioral intentions of an employee.

Please indicate your level of agreement with the following items or statements:

1. Ethical guidance provided to employees by an organization is an effective method of achieving desired behavior.
2. The actions of senior managers have no influence on whether employees conform to organizational policies or rules. (R)
3. Rewards and punishment are effective incentives for achieving compliance with organizational expectations.
4. Cost, schedule, and performance requirements do not affect employee compliance with business requirements. (R)
5. The morale level (esprit de corps) of an organization does not play a role in employee behavior. (R)
6. An individual’s actions may be dictated by their religious beliefs.
7. A person’s opinion of what is acceptable behavior is affected by their cultural background.
8. Personal factors or variables such as age, gender, and life experiences contribute very little to an individual’s concept of “right” behavior. (R)
9. An individual’s ethical foundation is unaffected by their participation in social organizations. (R)

10. Friends and peers impact a person’s sense of right and wrong behavior.

11. Events in an employee’s personal life can affect their behavior at work.

12. An employee’s personal beliefs play a role in how they react to an organization's behavioral guidelines.

F. The following is a list of items that may be considered to be examples or results of employee ethical behavior in regards to information system security.

What is your level of agreement that the following items are indicators of ethical behavior?

1. Employees follow organizational policies and rules when making decisions regarding information system security.
2. In the absence of specific organizational guidance employees may deviate from information system security best practices. (R)
3. An organization experiencing a reduction in the number of events involving loss or compromise of information is an indicator of employee ethical behavior.
4. Employees exhibit concern with the well-being of the organization by protecting organizational information and information technology assets.
5. An example of ethical behavior is when employees feel uncomfortable in disclosing security issues if they believe that other employees or the organization may disagree with them. (R)

G. Thank you very much for taking the time to participate. You are encouraged to invite other information systems security professionals to participate in this survey. Please feel free to forward the survey URL to qualified individuals.

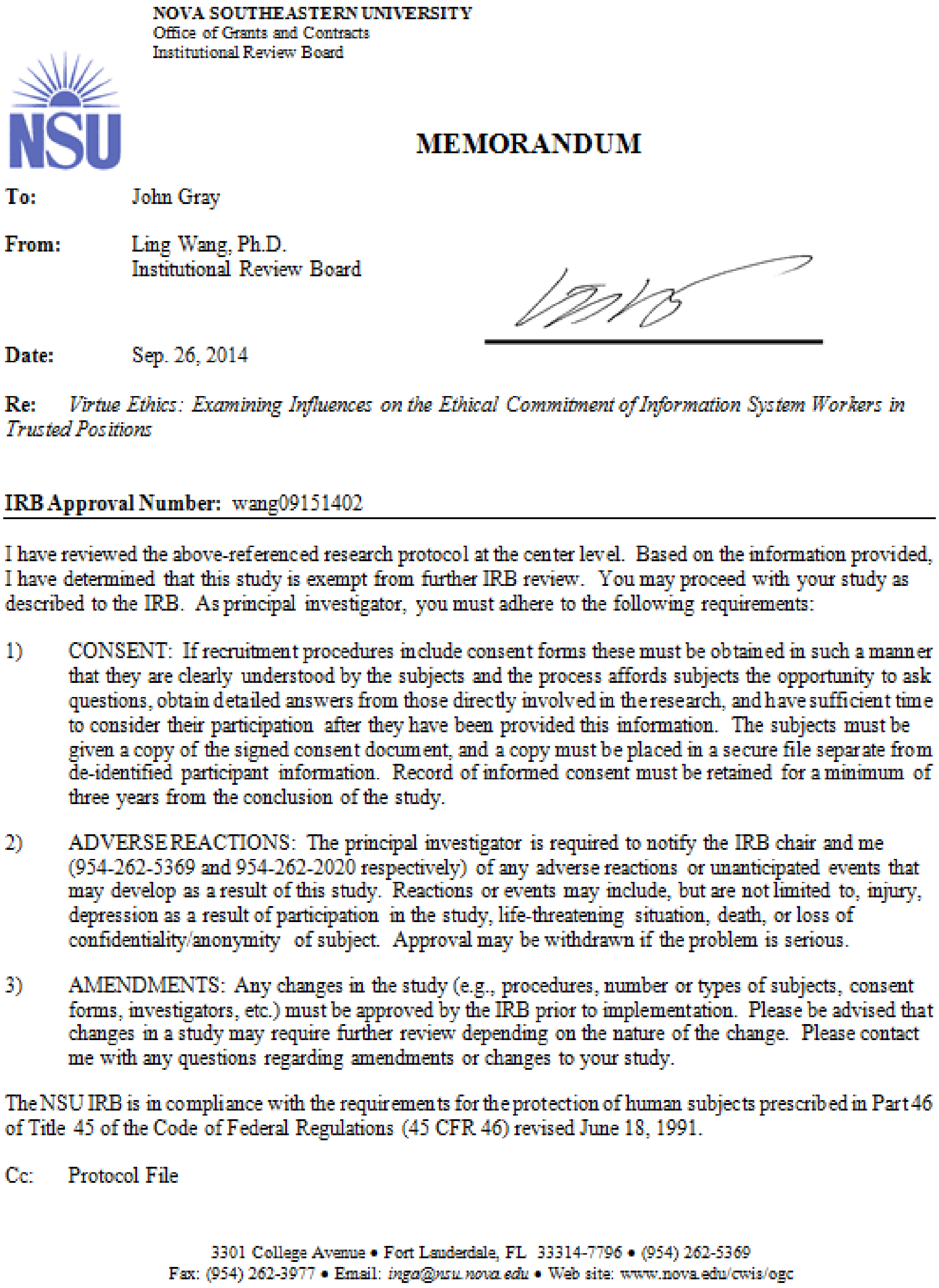
Do you have any feedback, comments, or recommendations for improvement regarding this survey?

If you are willing to help improve the quality and validity of the survey results by participating in a retest of the survey at a later date, please provide an email address that the follow-up survey url can be emailed to.

The follow-up survey will be emailed to you in approximately 30 days.

Appendix D

IRB Approval from Nova Southeastern University



NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: John Gray

From: Ling Wang, Ph.D.
Institutional Review Board

Date: Sep. 26, 2014

Re: *Virtue Ethics: Examining Influences on the Ethical Commitment of Information System Workers in Trusted Positions*

IRB Approval Number: wang09151402

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

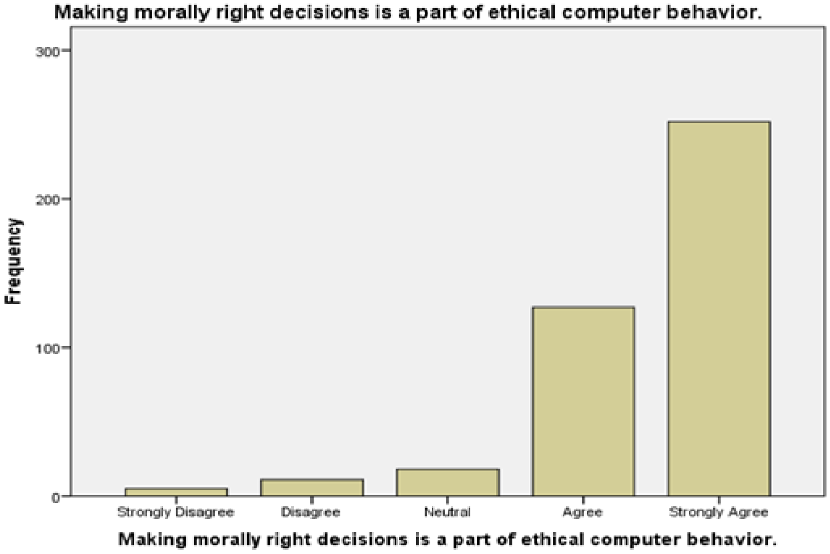
3301 College Avenue • Fort Lauderdale, FL 33314-7796 • (954) 262-5369
Fax: (954) 262-3977 • Email: *inga@nsu.nova.edu* • Web site: www.nova.edu/cwis/ogc

Appendix E

Survey Response Frequency and Percentage Information

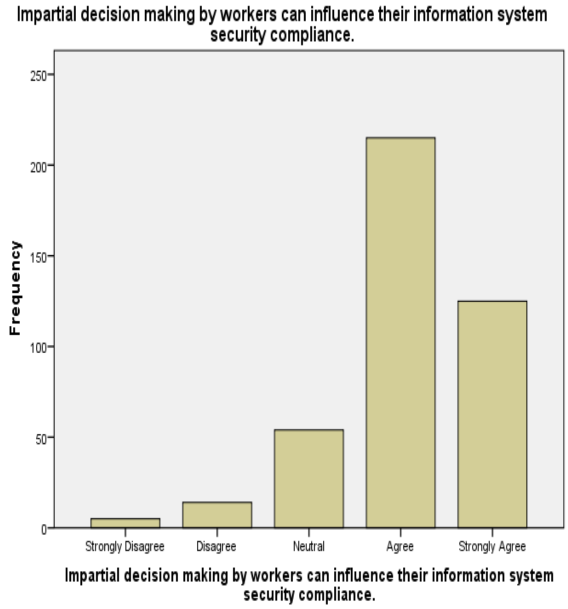
Research Model Variable: ISS Astuteness

Observable Indicator Identifier: AS1



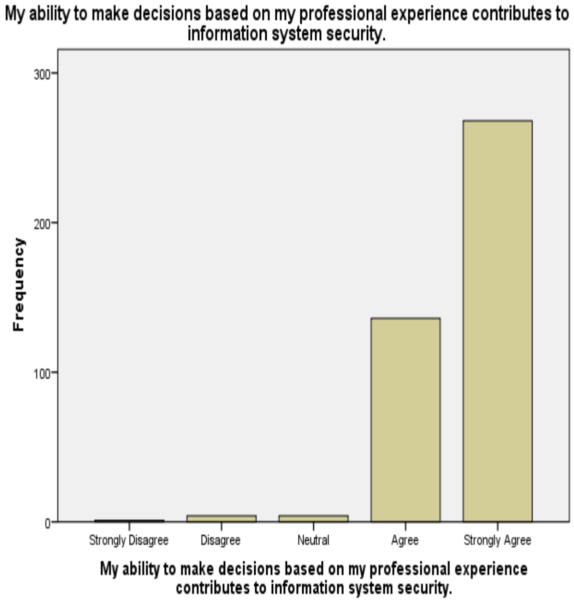
Response	Frequency	Valid Percent
Strongly Disagree	5	1.2
Disagree	11	2.7
Neutral	18	4.4
Agree	127	30.8
Strongly Agree	252	61.0
Total	413	100.0

Observable Indicator Identifier: AS2



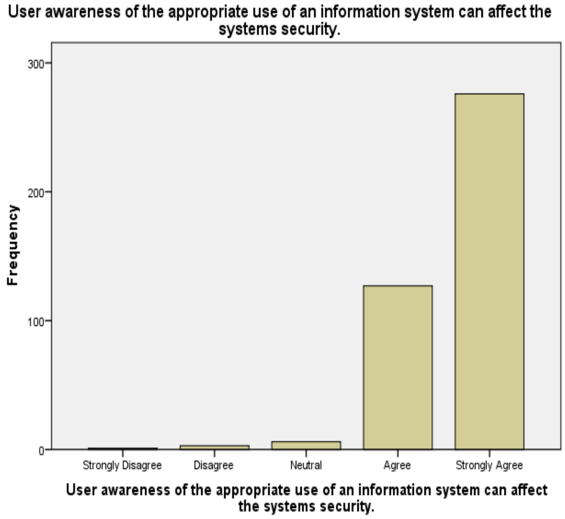
Response	Frequency	Valid Percent
Strongly Disagree	5	1.2
Disagree	14	3.4
Neutral	54	13.1
Agree	215	52.1
Strongly Agree	125	30.3
Total	413	100.0

Observable Indicator Identifier: AS3



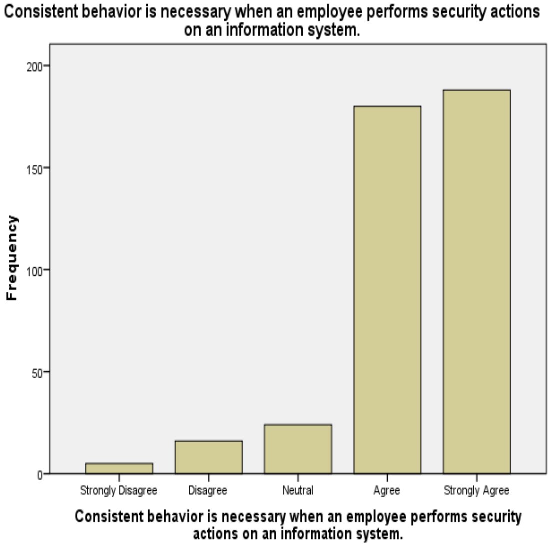
Response	Frequency	Valid Percent
Strongly Disagree	1	.2
Disagree	4	1.0
Neutral	4	1.0
Agree	136	32.9
Strongly Agree	268	64.9
Total	413	100.0

Observable Indicator Identifier: AS4



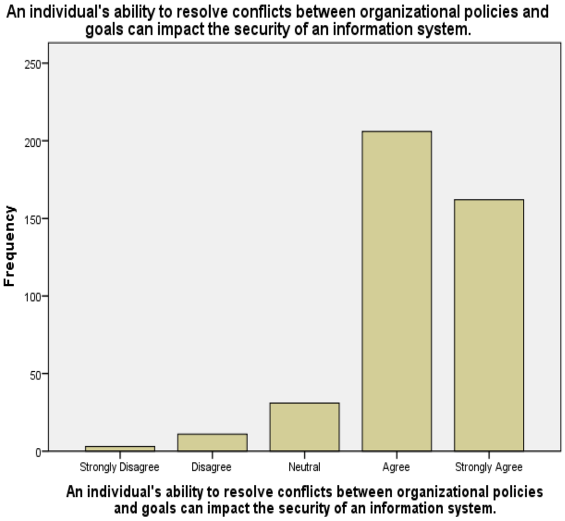
Response	Frequency	Valid Percent
Strongly Disagree	1	.2
Disagree	3	.7
Neutral	6	1.5
Agree	127	30.8
Strongly Agree	276	66.8
Total	413	100.0

Observable Indicator Identifier: AS5



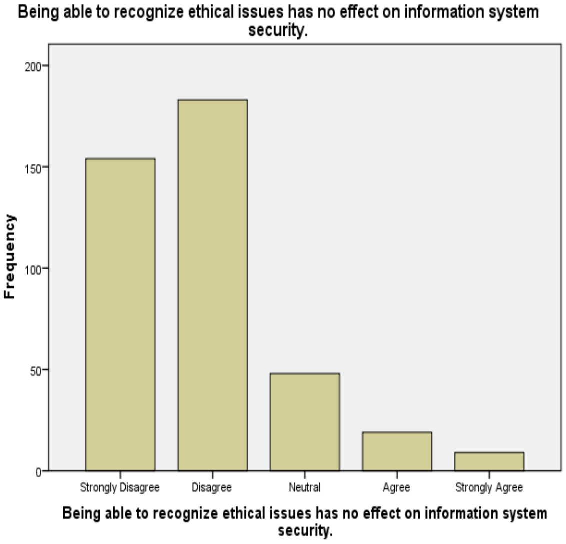
Response	Frequency	Valid Percent
Strongly Disagree	5	1.2
Disagree	16	3.9
Neutral	24	5.8
Agree	180	43.6
Strongly Agree	188	45.5
Total	413	100.0

Observable Indicator Identifier: AS6



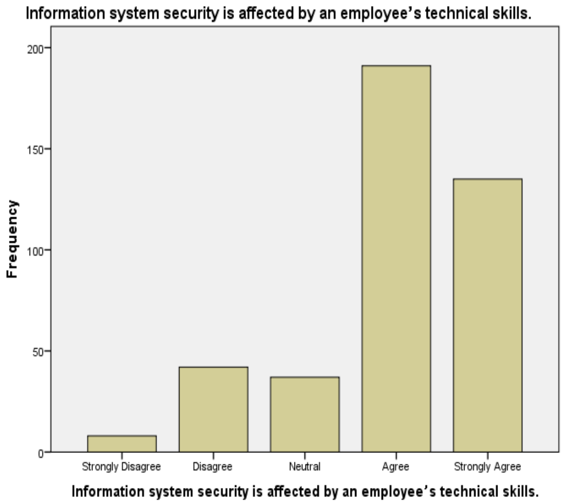
Response	Frequency	Valid Percent
Strongly Disagree	3	.7
Disagree	11	2.7
Neutral	31	7.5
Agree	206	49.9
Strongly Agree	162	39.2
Total	413	100.0

Observable Indicator Identifier: AS7



Response	Frequency	Valid Percent
Strongly Disagree	154	37.3
Disagree	183	44.3
Neutral	48	11.6
Agree	19	4.6
Strongly Agree	9	2.2
Total	413	100.0

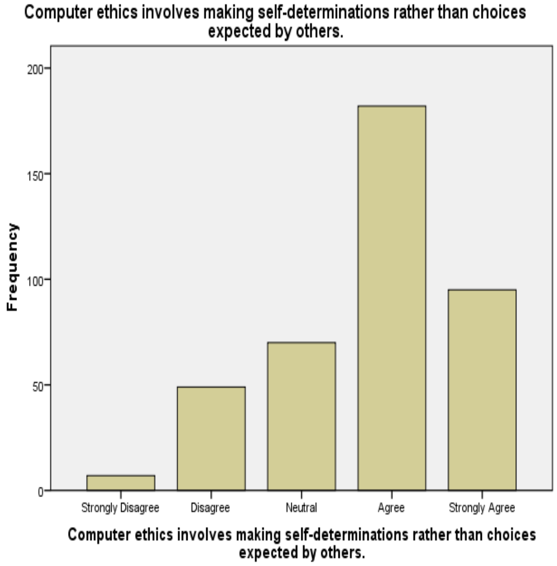
Observable Indicator Identifier: AS8



Response	Frequency	Valid Percent
Strongly Disagree	8	1.9
Disagree	42	10.2
Neutral	37	9.0
Agree	191	46.2
Strongly Agree	135	32.7
Total	413	100.0

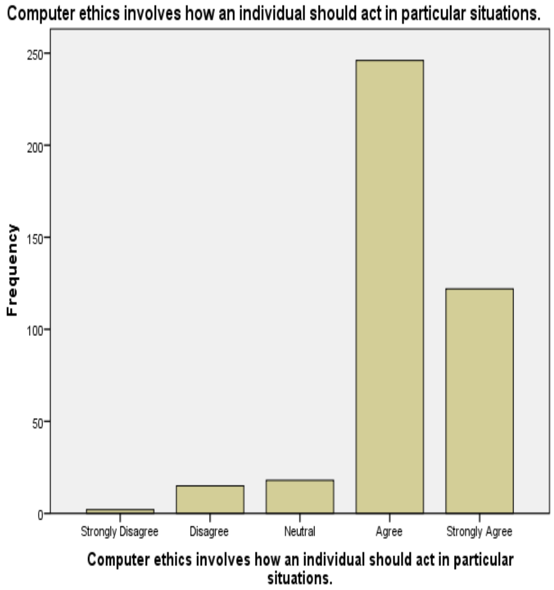
Research Model Variable: ISS Conviction

Observable Indicator Identifier: CO1



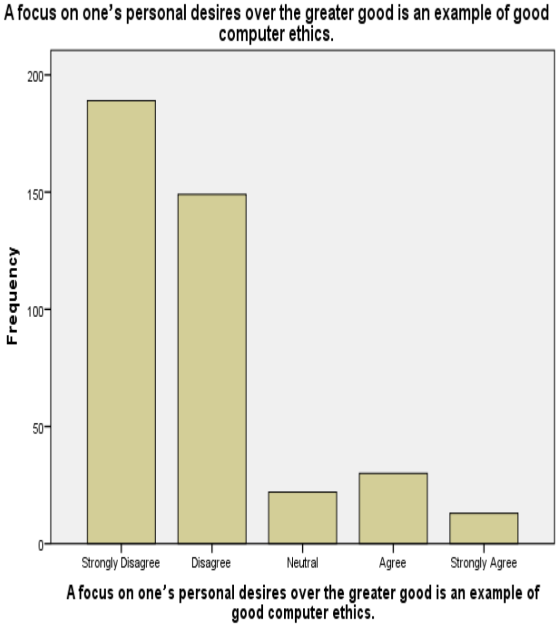
Response	Frequency	Valid Percent
Strongly Disagree	7	1.7
Disagree	49	12.2
Neutral	70	17.4
Agree	182	45.2
Strongly Agree	95	23.6
Total	403	100.0

Observable Indicator Identifier: CO2



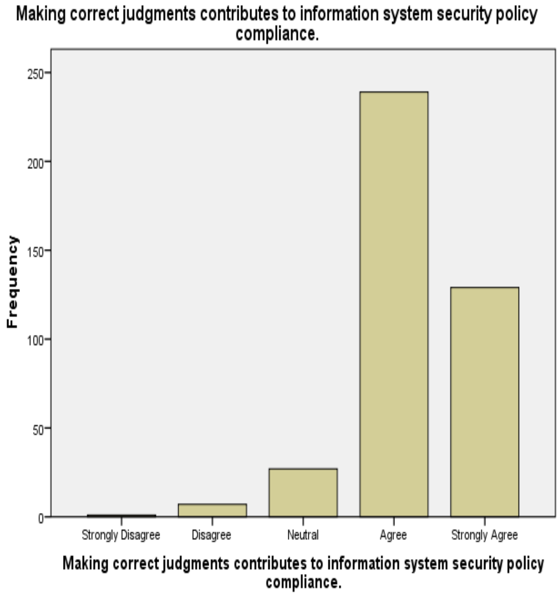
Response	Frequency	Valid Percent
Strongly Disagree	2	.5
Disagree	15	3.7
Neutral	18	4.5
Agree	246	61.0
Strongly Agree	122	30.3
Total	403	100.0

Observable Indicator Identifier: CO3



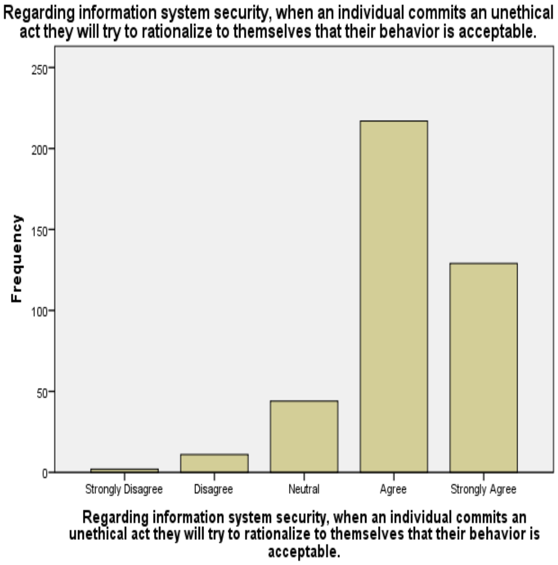
Response	Frequency	Valid Percent
Strongly Disagree	189	46.9
Disagree	149	37.0
Neutral	22	5.5
Agree	30	7.4
Strongly Agree	13	3.2
Total	403	100.0

Observable Indicator Identifier: CO4



Response	Frequency	Valid Percent
Strongly Disagree	1	.2
Disagree	7	1.7
Neutral	27	6.7
Agree	239	59.3
Strongly Agree	129	32.0
Total	403	100.0

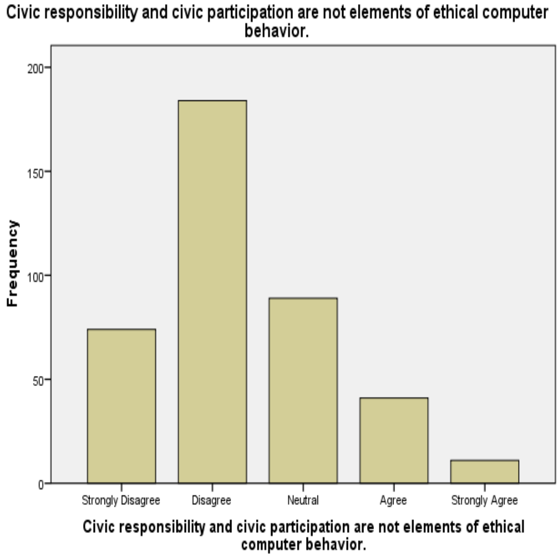
Observable Indicator Identifier: CO5



Response	Frequency	Valid Percent
Strongly Disagree	2	.5
Disagree	11	2.7
Neutral	44	10.9
Agree	217	53.8
Strongly Agree	129	32.0
Total	403	100.0

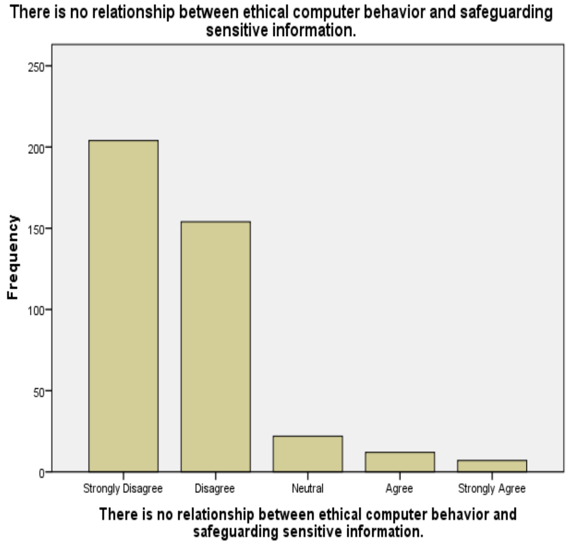
Research Model Variable: ISS Rectitude

Observable Indicator Identifier: RE1



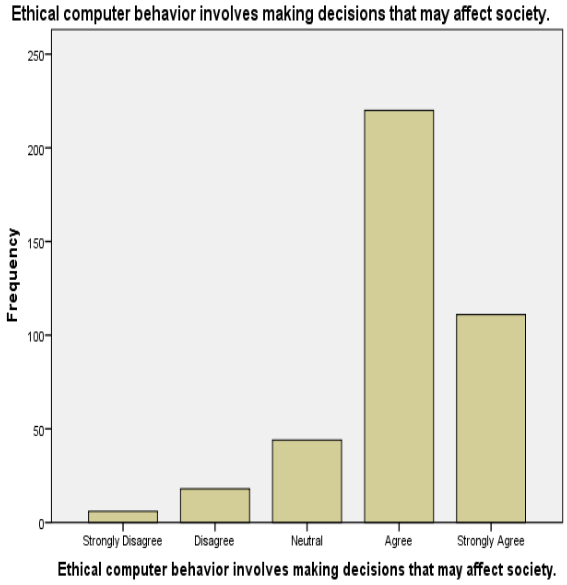
Response	Frequency	Valid Percent
Strongly Disagree	74	18.5
Disagree	184	46.1
Neutral	89	22.3
Agree	41	10.3
Strongly Agree	11	2.8
Total	399	100.0

Observable Indicator Identifier: RE2



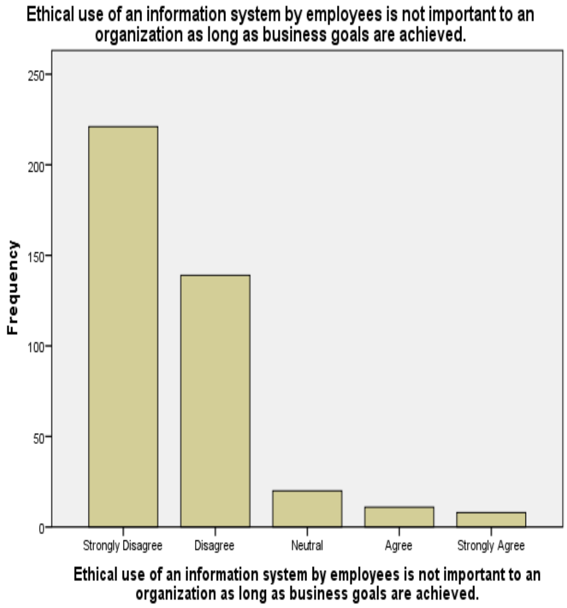
Response	Frequency	Valid Percent
Strongly Disagree	204	51.1
Disagree	154	38.6
Neutral	22	5.5
Agree	12	3.0
Strongly Agree	7	1.8
Total	399	100.0

Observable Indicator Identifier: RE3



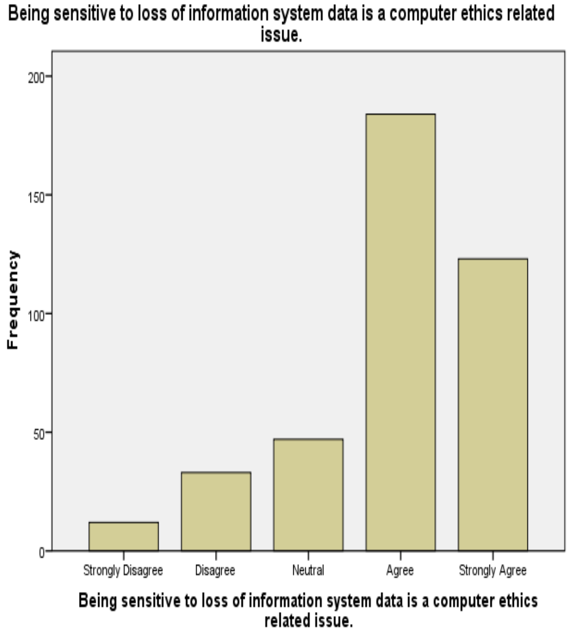
Response	Frequency	Valid Percent
Strongly Disagree	6	1.5
Disagree	18	4.5
Neutral	44	11.0
Agree	220	55.1
Strongly Agree	111	27.8
Total	399	100.0

Observable Indicator Identifier: RE4



Response	Frequency	Valid Percent
Strongly Disagree	221	55.4
Disagree	139	34.8
Neutral	20	5.0
Agree	11	2.8
Strongly Agree	8	2.0
Total	399	100.0

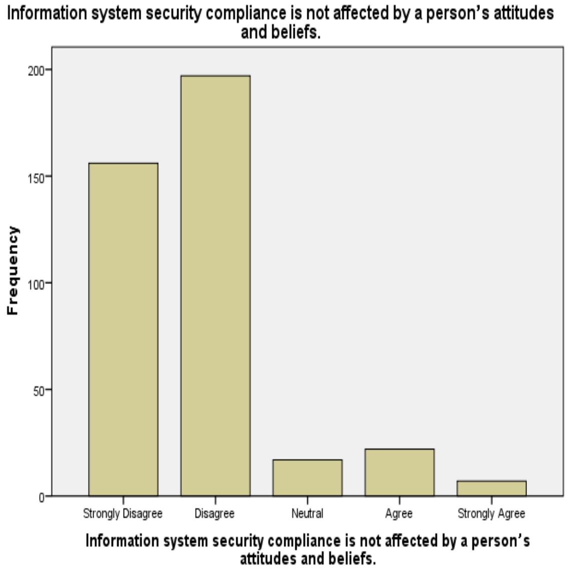
Observable Indicator Identifier: RE5



Response	Frequency	Valid Percent
Strongly Disagree	12	3.0
Disagree	33	8.3
Neutral	47	11.8
Agree	184	46.1
Strongly Agree	123	30.8
Total	399	100.0

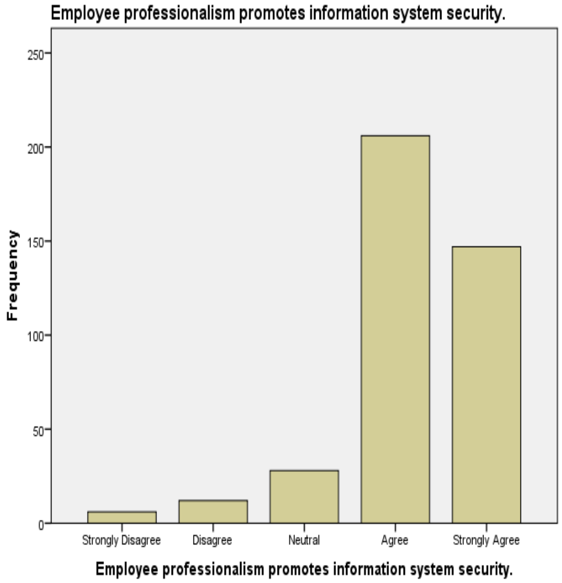
Research Model Variable: ISS Self-Discipline

Observable Indicator Identifier: SD1



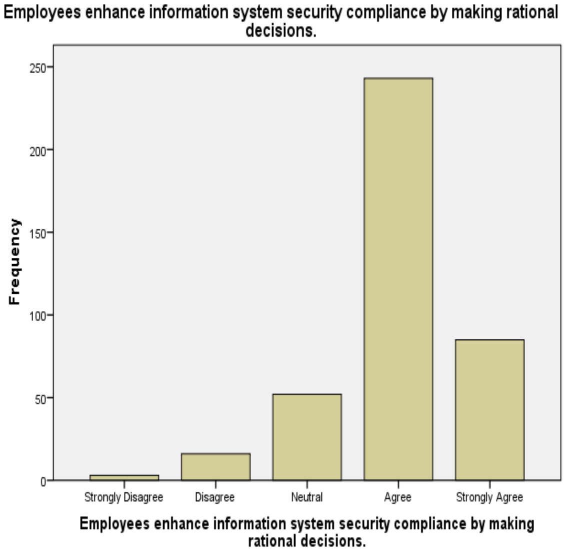
Response	Frequency	Valid Percent
Strongly Disagree	156	39.1
Disagree	197	49.4
Neutral	17	4.3
Agree	22	5.5
Strongly Agree	7	1.8
Total	399	100.0

Observable Indicator Identifier: SD2



Response	Frequency	Valid Percent
Strongly Disagree	6	1.5
Disagree	12	3.0
Neutral	28	7.0
Agree	206	51.6
Strongly Agree	147	36.8
Total	399	100.0

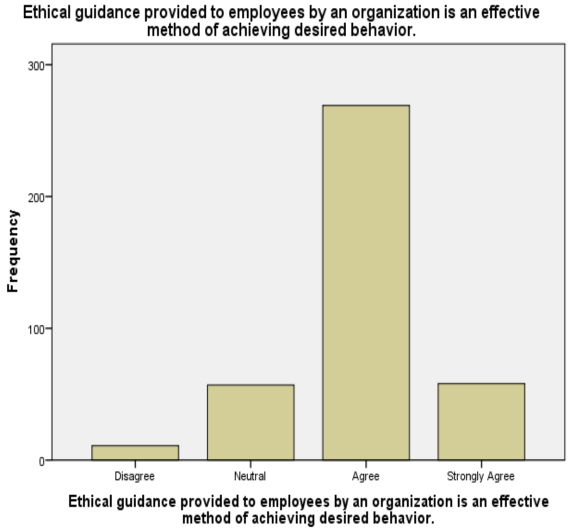
Observable Indicator Identifier: SD3



Response	Frequency	Valid Percent
Strongly Disagree	3	.8
Disagree	16	4.0
Neutral	52	13.0
Agree	243	60.9
Strongly Agree	85	21.3
Total	399	100.0

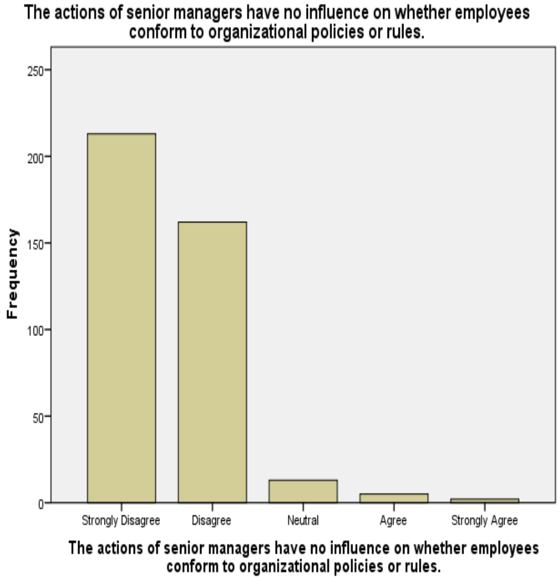
Research Model Variable: Internal Influences

Observable Indicator Identifier: II1



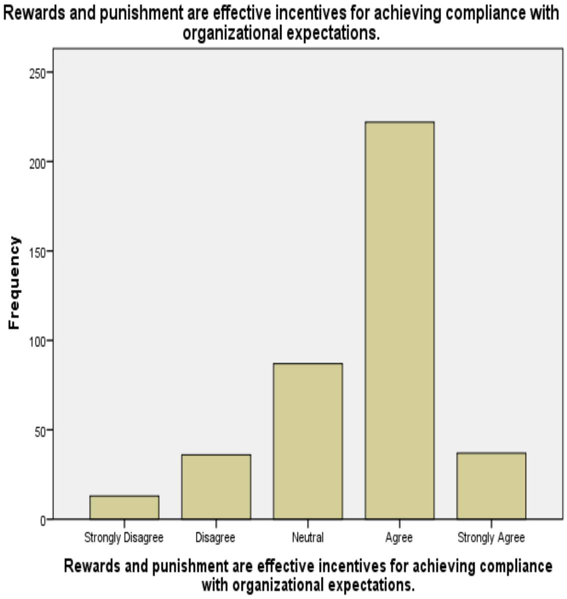
Response	Frequency	Valid Percent
Strongly Disagree	0	0
Disagree	11	2.8
Neutral	57	14.4
Agree	269	68.1
Strongly Agree	58	14.7
Total	395	100.0

Observable Indicator Identifier: II2



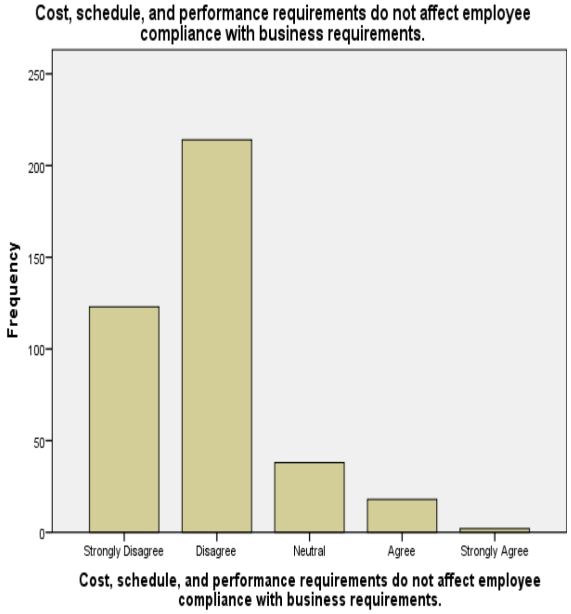
Response	Frequency	Valid Percent
Strongly Disagree	213	53.9
Disagree	162	41.0
Neutral	13	3.3
Agree	5	1.3
Strongly Agree	2	.5
Total	395	100.0

Observable Indicator Identifier: II3



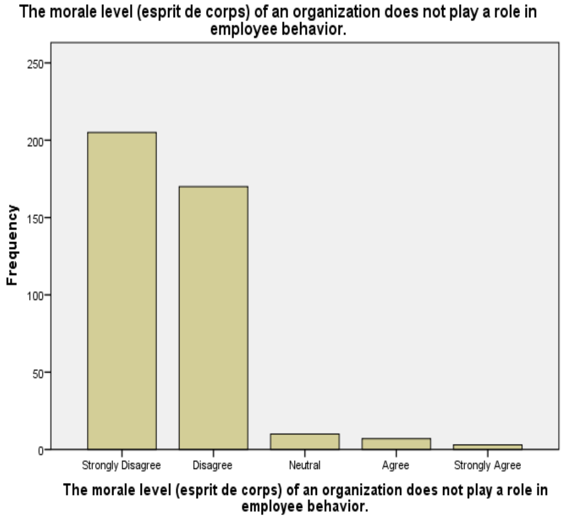
Response	Frequency	Valid Percent
Strongly Disagree	13	3.3
Disagree	36	9.1
Neutral	87	22.0
Agree	222	56.2
Strongly Agree	37	9.4
Total	395	100.0

Observable Indicator Identifier: II4



Response	Frequency	Valid Percent
Strongly Disagree	123	31.1
Disagree	214	54.2
Neutral	38	9.6
Agree	18	4.6
Strongly Agree	2	.5
Total	395	100.0

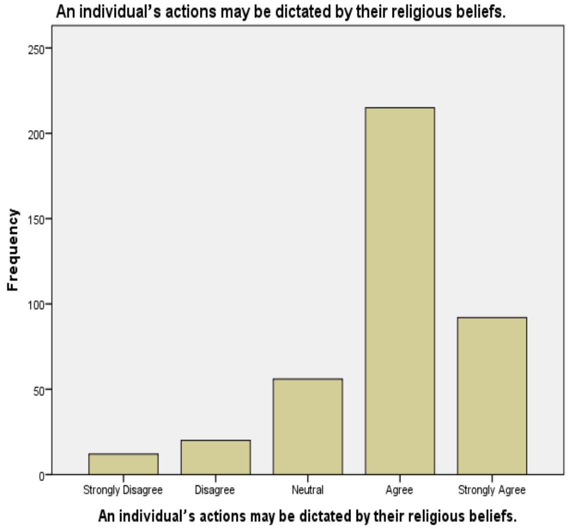
Observable Indicator Identifier: II5



Response	Frequency	Valid Percent
Strongly Disagree	205	51.9
Disagree	170	43.0
Neutral	10	2.5
Agree	7	1.8
Strongly Agree	3	.8
Total	395	100.0

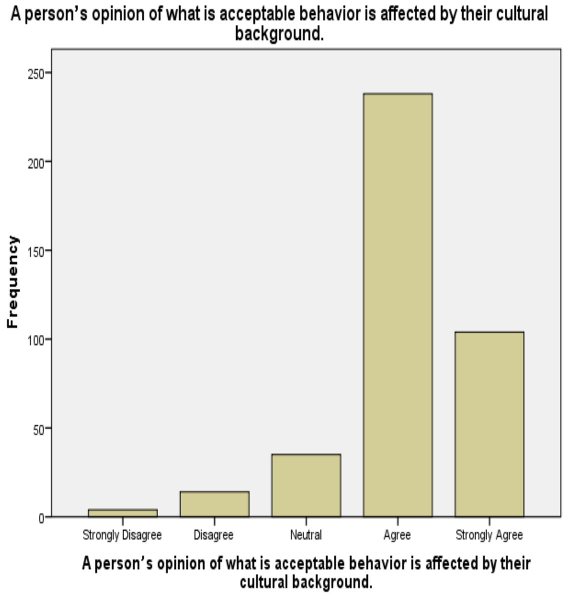
Research Model Variable: External Influences

Observable Indicator Identifier: EI1



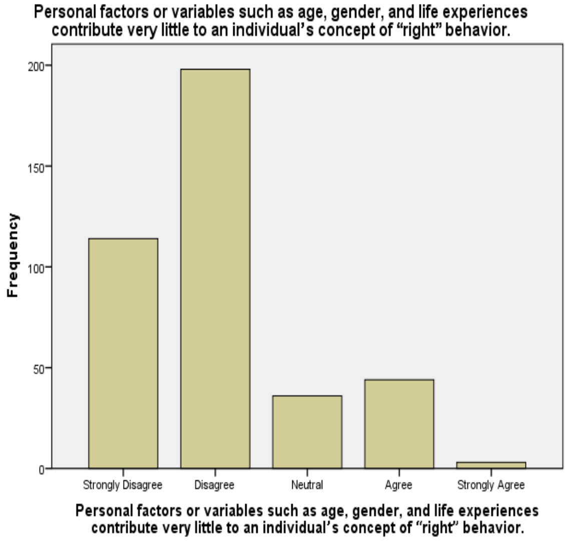
Response	Frequency	Valid Percent
Strongly Disagree	12	3.0
Disagree	20	5.1
Neutral	56	14.2
Agree	215	54.4
Strongly Agree	92	23.3
Total	395	100.0

Observable Indicator Identifier: EI2



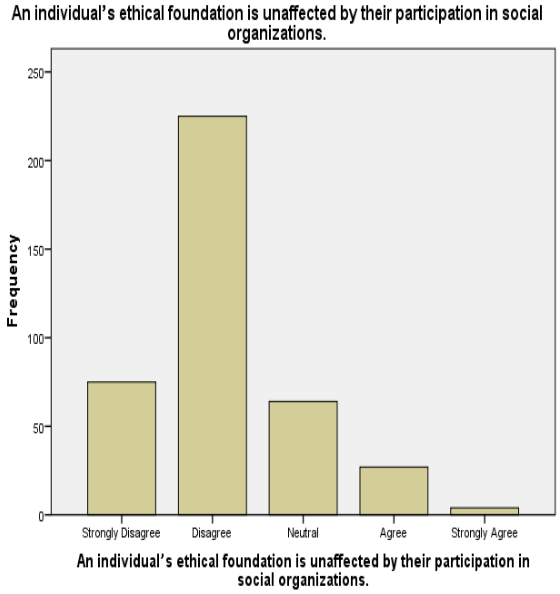
Response	Frequency	Valid Percent
Strongly Disagree	4	1.0
Disagree	14	3.5
Neutral	35	8.9
Agree	238	60.3
Strongly Agree	104	26.3
Total	395	100.0

Observable Indicator Identifier: EI3



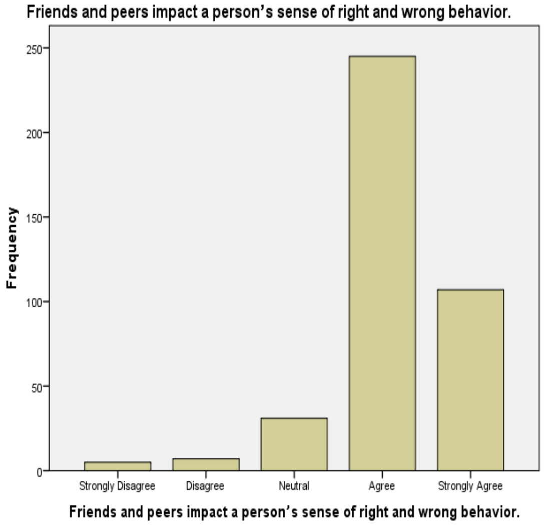
Response	Frequency	Valid Percent
Strongly Disagree	114	28.9
Disagree	198	50.1
Neutral	36	9.1
Agree	44	11.1
Strongly Agree	3	.8
Total	395	100.0

Observable Indicator Identifier: EI4



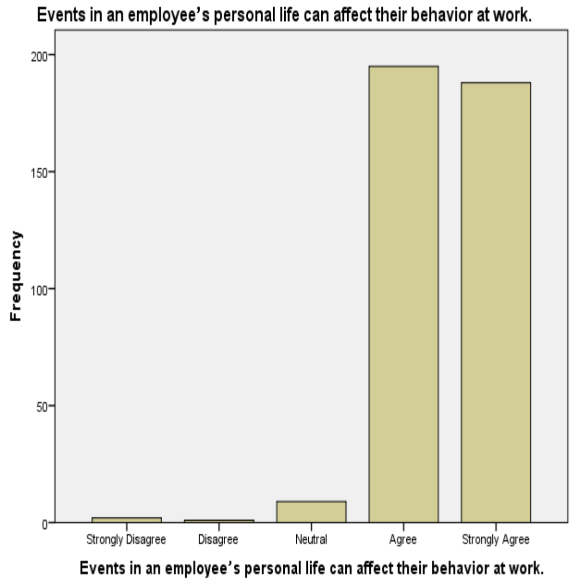
Response	Frequency	Valid Percent
Strongly Disagree	75	19.0
Disagree	225	57.0
Neutral	64	16.2
Agree	27	6.8
Strongly Agree	4	1.0
Total	395	100.0

Observable Indicator Identifier: EI5



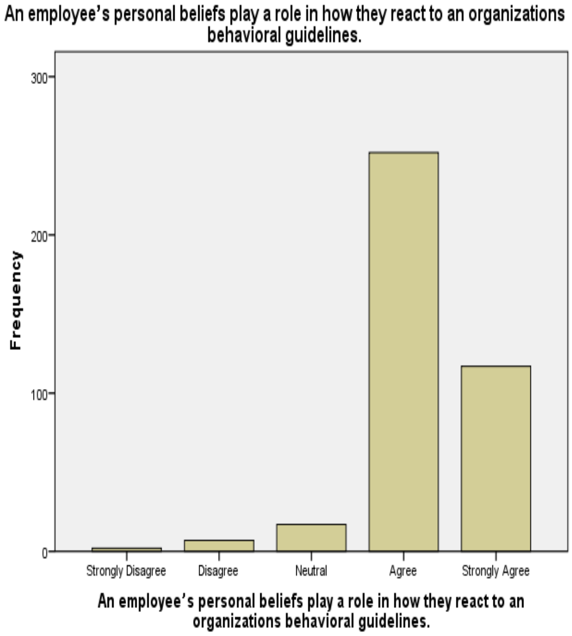
Response	Frequency	Valid Percent
Strongly Disagree	5	1.3
Disagree	7	1.8
Neutral	31	7.8
Agree	245	62.0
Strongly Agree	107	27.1
Total	395	100.0

Observable Indicator Identifier: EI6



Response	Frequency	Valid Percent
Strongly Disagree	2	.5
Disagree	1	.3
Neutral	9	2.3
Agree	195	49.4
Strongly Agree	188	47.6
Total	395	100.0

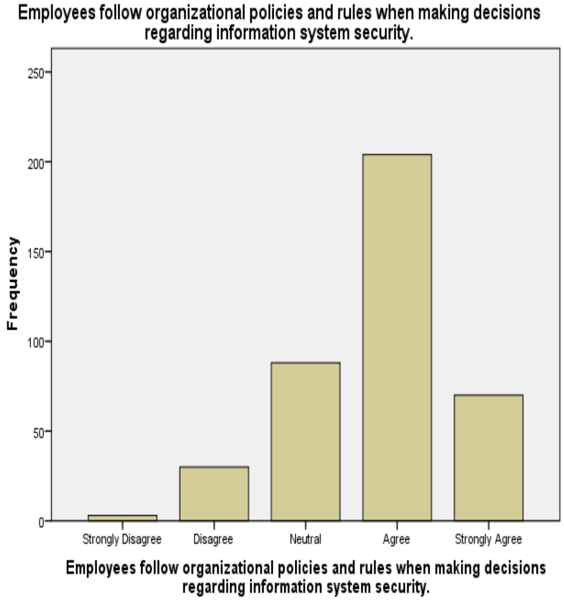
Observable Indicator Identifier: EI7



Response	Frequency	Valid Percent
Strongly Disagree	2	.5
Disagree	7	1.8
Neutral	17	4.3
Agree	252	63.8
Strongly Agree	117	29.6
Total	395	100.0

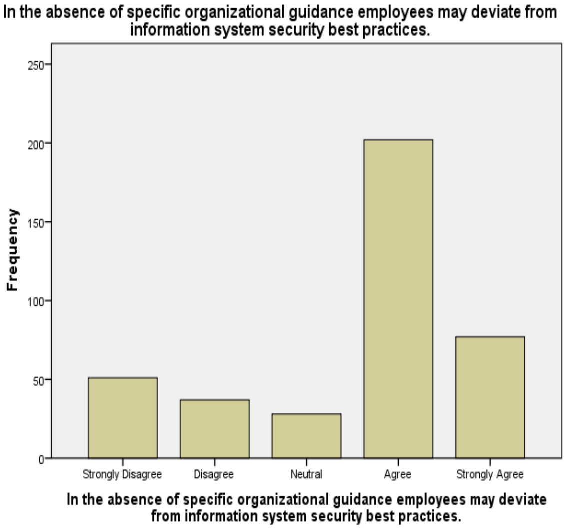
Research Model Variable: Ethical Behavior

Observable Indicator Identifier: EB1



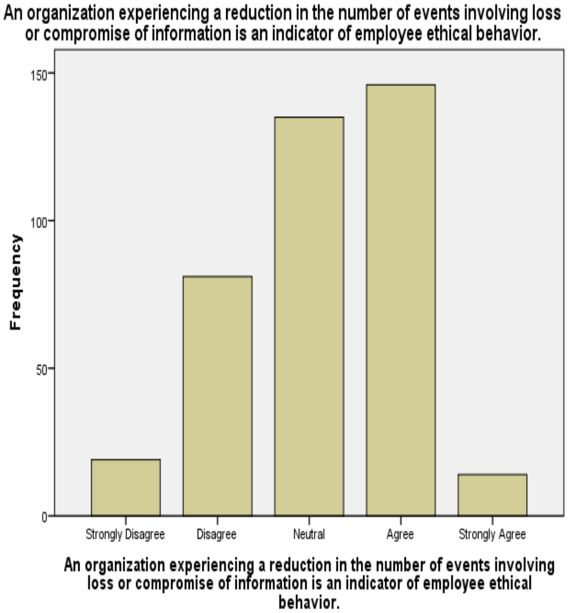
Response	Frequency	Valid Percent
Strongly Disagree	3	.8
Disagree	30	7.6
Neutral	88	22.3
Agree	204	51.6
Strongly Agree	70	17.7
Total	395	100.0

Observable Indicator Identifier: EB2



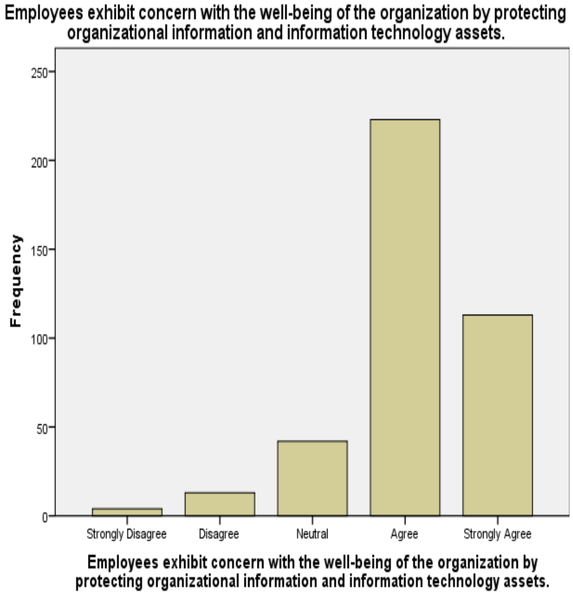
Response	Frequency	Valid Percent
Strongly Disagree	51	12.9
Disagree	37	9.4
Neutral	28	7.1
Agree	202	51.1
Strongly Agree	77	19.5
Total	395	100.0

Observable Indicator Identifier: EB3



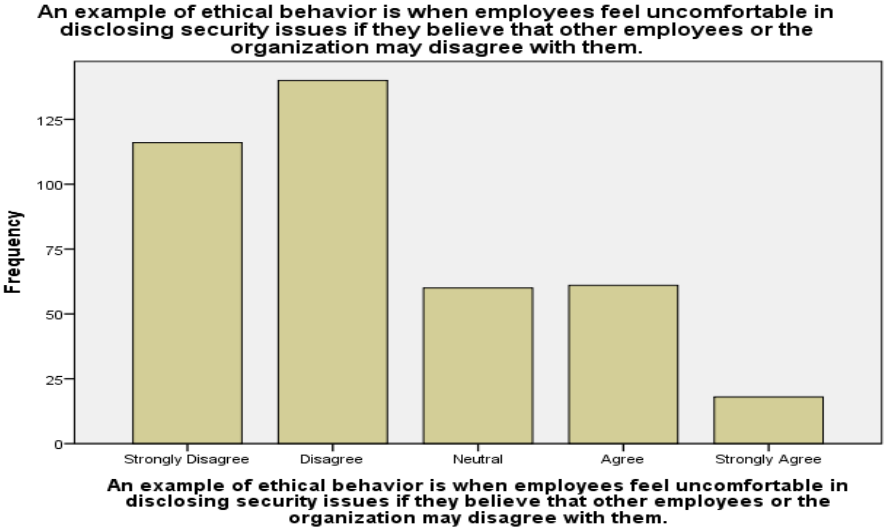
Response	Frequency	Valid Percent
Strongly Disagree	19	4.8
Disagree	81	20.5
Neutral	135	34.2
Agree	146	37.0
Strongly Agree	14	3.5
Total	395	100.0

Observable Indicator Identifier: EB4



Response	Frequency	Valid Percent
Strongly Disagree	4	1.0
Disagree	13	3.3
Neutral	42	10.6
Agree	223	56.5
Strongly Agree	113	28.6
Total	395	100.0

Observable Indicator Identifier: EB5

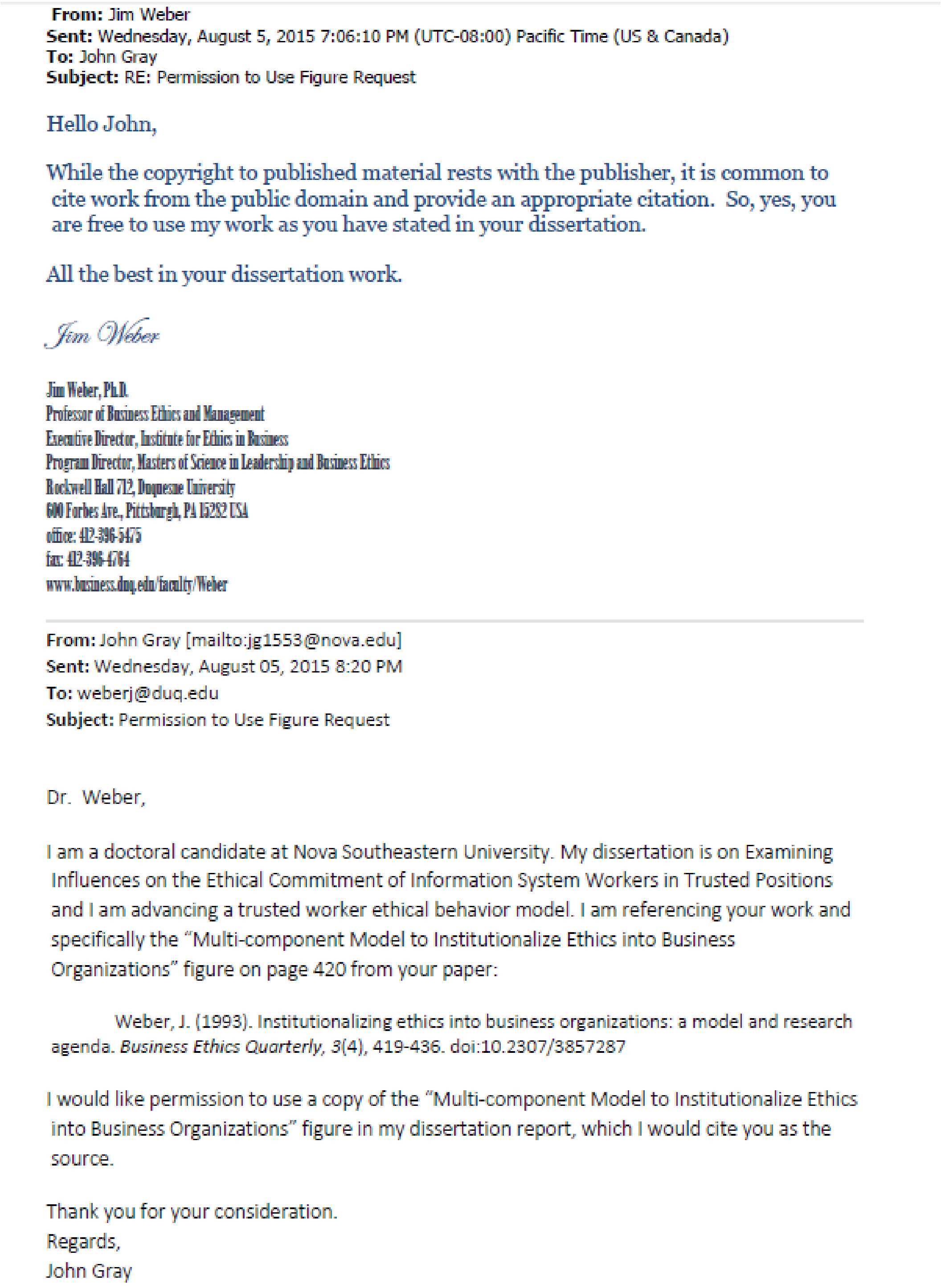


Response	Frequency	Valid Percent
Strongly Disagree	116	29.4
Disagree	140	35.4
Neutral	60	15.2
Agree	61	15.4
Strongly Agree	18	4.6
Total	395	100.0

Appendix F

Copyright Permissions

Figure 2: Multi-component Model to Institutionalize Ethics into Business Organizations



From: Jim Weber
Sent: Wednesday, August 5, 2015 7:06:10 PM (UTC-08:00) Pacific Time (US & Canada)
To: John Gray
Subject: RE: Permission to Use Figure Request

Hello John,

While the copyright to published material rests with the publisher, it is common to cite work from the public domain and provide an appropriate citation. So, yes, you are free to use my work as you have stated in your dissertation.

All the best in your dissertation work.

Jim Weber

Jim Weber, Ph.D.
Professor of Business Ethics and Management
Executive Director, Institute for Ethics in Business
Program Director, Masters of Science in Leadership and Business Ethics
Rockwell Hall 712, Duquesne University
600 Forbes Ave., Pittsburgh, PA 15282 USA
office: 412-396-5475
fax: 412-396-4764
www.business.duq.edu/faculty/Weber

From: John Gray [mailto:jg1553@nova.edu]
Sent: Wednesday, August 05, 2015 8:20 PM
To: weberj@duq.edu
Subject: Permission to Use Figure Request

Dr. Weber,

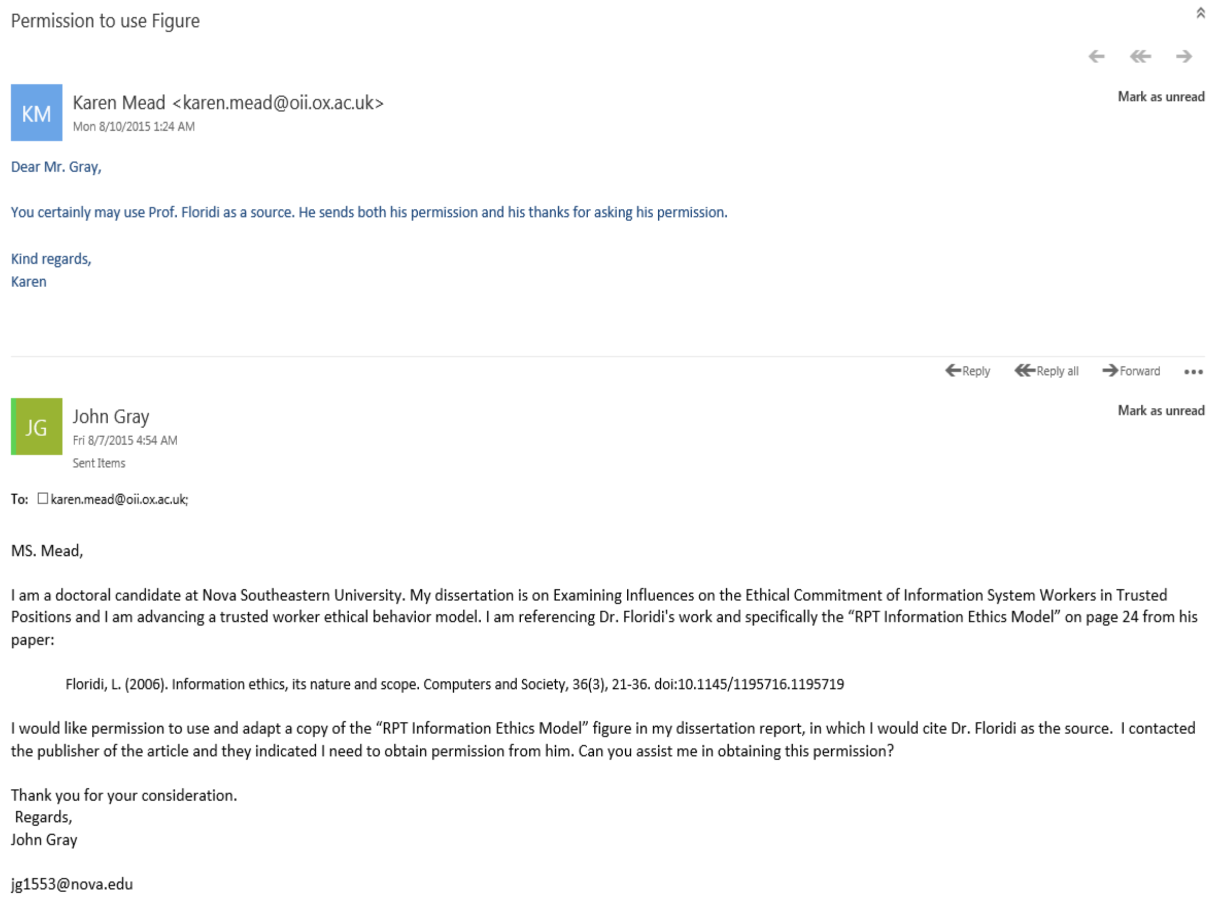
I am a doctoral candidate at Nova Southeastern University. My dissertation is on Examining Influences on the Ethical Commitment of Information System Workers in Trusted Positions and I am advancing a trusted worker ethical behavior model. I am referencing your work and specifically the "Multi-component Model to Institutionalize Ethics into Business Organizations" figure on page 420 from your paper:

Weber, J. (1993). Institutionalizing ethics into business organizations: a model and research agenda. *Business Ethics Quarterly*, *3*(4), 419-436. doi:10.2307/3857287

I would like permission to use a copy of the "Multi-component Model to Institutionalize Ethics into Business Organizations" figure in my dissertation report, which I would cite you as the source.

Thank you for your consideration.
Regards,
John Gray

Figure 3: RPT Information Ethics Model



Permission to use Figure

KM Karen Mead <karen.mead@oii.ox.ac.uk>
Mon 8/10/2015 1:24 AM

Dear Mr. Gray,

You certainly may use Prof. Floridi as a source. He sends both his permission and his thanks for asking his permission.

Kind regards,
Karen

JG John Gray
Fri 8/7/2015 4:54 AM
Sent Items

To: □ karen.mead@oii.ox.ac.uk;

MS. Mead,

I am a doctoral candidate at Nova Southeastern University. My dissertation is on Examining Influences on the Ethical Commitment of Information System Workers in Trusted Positions and I am advancing a trusted worker ethical behavior model. I am referencing Dr. Floridi's work and specifically the “RPT Information Ethics Model” on page 24 from his paper:

> Floridi, L. (2006). Information ethics, its nature and scope. Computers and Society, 36(3), 21-36. doi:10.1145/1195716.1195719

I would like permission to use and adapt a copy of the “RPT Information Ethics Model” figure in my dissertation report, in which I would cite Dr. Floridi as the source. I contacted the publisher of the article and they indicated I need to obtain permission from him. Can you assist me in obtaining this permission?

Thank you for your consideration.
Regards,
John Gray

jg1553@nova.edu

Ms. Karen Mead is Dr. Floridi’s personal assistant at the University of Oxford

Figure 7: Scale Development Procedure

MANAGEMENT INFORMATION SYSTEMS QUARTERLY

Order detail ID:	67900731
Order License Id:	3682610000039
ISSN:	0276-7783
Publication Type:	Journal
Volume:	
Issue:	
Start page:	
Publisher:	M I S RESEARCH CENTER
Author/Editor:	SOCIETY FOR INFORMATION MANAGEMENT (U.S.) ; UNIVERSITY OF MINNESOTA ; SOCIETY FOR MANAGEMENT INFORMATION SYSTEMS (U.S.)

Permission Status: ✓ **Granted**

Permission type:	Republish or display content
Type of use:	Thesis/Dissertation

⊟ Hide details

Requestor type	Author of requested content
Format	Print, Electronic
Portion	chart/graph/table/figure
Number of charts/graphs/tables/figures	1
Title or numeric reference of the portion(s)	Figure 1: Scale Development Procedure
Title of the article or chapter the portion is from	Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques
Editor of portion(s)	n/a
Author of portion(s)	MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P.
Volume of serial or monograph	35
Issue, if republishing an article from a serial	2
Page range of portion	297
Publication date of portion	2011
Rights for	Main product
Duration of use	Current edition and up to 5 years
Creation of copies for the disabled	no
With minor editing privileges	no
For distribution to	United States
In the following language(s)	Original language of publication
With incidental promotional use	no

References

Adam, A., & Bull, C. (2008). Exploring MacIntyre's virtue ethics in relation to information systems. *European Conference on Information Systems (ECIS), Galway, Ireland,* 1-11.

Adams, J. S., Tashchian, A., & Shore, T. H. (2001). Codes of ethics as signals for ethical behavior. *Journal of Business Ethics, 29*(3), 199-211. doi: 10.1023/A:1026576421399

Adler, N. J. (1983). A typology of management studies involving culture. *Journal of International Business Studies*, *14*(2), 29-47. doi:10.1057/palgrave.jibs.8490517

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi:10.1016/0749-5978(91)90020-T

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A behavior compliance conceptual framework. *Proceedings of the 8th Australasian Information Security Conference (AISC 2010), Brisbane, Australia*, 47-55.

Althebyan, Q., & Panda, B. (2007). A knowledge-base model for insider threat prediction. *Proceedings of the 2007 IEEE Information Assurance and Security Workshop (IAW'07), West Point, NY*, 239-246. doi:10.1109/IAW.2007.381939

Ambrose, M. L., Arnaud, A., & Schminke, M. (2008). Individual moral development and ethical climate: The influence of person–organization fit on job attitudes. *Journal of Business Ethics*, *77*(3), 323-333. doi:10.1007/s10551-007-9352-1

Amorosi, D. (2011). WikiLeaks 'Cablegate' dominates year-end headlines. *Infosecurity, 8*(1), 6-9. doi:10.1016/S1754-4548(11)70002-X

Anderson, J. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308-313. doi:10.1016/S0167-4048(03)00407-3

Andreoli, N., & Lefkowitz, J. (2009). Individual and organizational antecedents of misconduct in organizations. *Journal of Business Ethics*, *85*(3), 309-332. doi:10.1007/s10551-008-9772-6

Aquinas, T. St. (2005). *The cardinal virtues: Prudence, justice, fortitude, and temperance.* (R. J. Regan, Translator). Indianapolis, IN: Hackett Publishing (Original work titled Summa theological, written 1265-1274).

Aristotle. (2005*). Nicomanchean ethics.* (W. D. Ross, Translator). Original work published 350 BCE.

Arjoon, S. (2000). Virtue theory as a dynamic theory of business. *Journal of Business Ethics, 28*(2), 159-178. doi:10.1023/A:1006339112331

Artz, J. M. (1994). Virtue vs. utility: Alternative foundations for computer ethics. *Proceedings of the Conference on Ethics in the Computer Age, Gatlinburg, TN, USA,* 16–21. doi:10.1145/199544.199553

Avery, A. J., Savelyich, B. S. P., Sheikh, A., Cantrill, J., Morris, C. J., Fernando, B., Bainbridge, M., Horsfield, P., & Teasdale, S. (2005). Identifying and establishing consensus on the most important safety features of GP computer systems: A Delphi study. *Informatics in Primary Care, 13*(3), 3-11.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems, 5*, 2-9. doi: 10.1057/ejis.1996.7

Ball, G. A., Trevino, L. K., & Sims, H. P. (1994). Just and unjust punishment: Influences on subordinate performance and citizenship. *Academy of Management Journal*, *37*(2), 299-322. doi: 10.2307/256831

Balsmeier, P., & Kelly, J. (1996). The ethics of sentencing white-collar criminals. *Journal of Business Ethics, 15*(2), 143-152. doi:10.1007/BF00705582

Banerjee, D., Cronan, T. P., & Jones, T.W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quarterly, 22*(1), 31-60. doi:10.2307/249677

Barrett, P. (2007). Structural equation modelling: Adjudging model fit. *Personality and Individual differences, 42*(5), 815-824. doi: 10.1016/j.paid.2006.09.018

Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*, 121-130. doi:10.1057/ejis.1991.20

Bentler, P. M. (2007). On tests and indices for evaluating structural models. *Personality and Individual Differences*, *42*(5), 825-829. doi:10.1016/j.paid.2006.09.024

Bernard, R. (2007). Information lifecycle security risk assessment: A tool for closing security gaps. *Computers & Security, 26*(1), 26-30. doi: 10.1016/j.cose.2006.12.005

Bertino, E., & Sandhu, R. (2005). Database security-concepts, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing, 2*(1), 2-19. doi:10.1109/TDSC.2005.9

Bollen, K. A., & Lennox, R. (1991). Conventional wisdom on measurement: A structural equation perspective. *Psychological Bulletin, 110*(2), 305-314. doi: 10.1037//0033-2909.110.2.305

Boomsma, A. (2000). Reporting analyses of covariance structures. *Structural equation modeling, 7*(3), 461-483.

Boss, S. R., Kirsch, K. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Bragado, E. (2002). Sukimátem: Isabelo de los Reyes revisited. *Philippine Studies: Historical and Ethnographic Viewpoints, 50*(1), 50-74.

Bright, D. S., Winn, B. A., & Kanov, J. (2014). Reconsidering virtue: Differences of perspective in virtue ethics and the positive social sciences. *Journal of Business Ethics, 119*(4), 445-460.

Brown, J. D. (2011). Likert items and scales of measurement. *Shiken: JALT Testing & Evaluation SIG Newsletter, 15*(1), 10-14.

Brown, M. E., Trevino, L. K., & Harrison, D. A. (2005). Ethical leadership: A social learning perspective for construct development and testing. *Organizational behavior and human decision processes, 97*(2), 117-134. doi: 10.1016/j.obhdp.2005.03.002

Cartelli, A., Daltri, A., Errani, P., Palma, M., & Zanfini, P. (2009). The Open Catalogue of Manuscripts in the Malatestiana Library. In A. Cartelli, & M. Palma (Eds.), *Encyclopedia of Information Communication Technology* (pp. 656-661). Hershey, PA: Information Science Reference. doi:10.4018/978-1-59904-845-1.ch086

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS Quarterly, 33*(4), 689-708.

Cerza, A. (1968). Freemasonry Comes to Illinois. *Journal of the Illinois State Historical Society (1908-1984), 61*(2), 182-190.

Chandler, G. N., DeTienne, D. R., McKelvie, A., & Mumford, T. V. (2011). Causation and effectuation processes: A validation study. *Journal of Business Venturing, 26*(3), 375-390. doi:10.1016/j.jbusvent.2009.10.006

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing security management. *Industrial Management and Data Systems, 106*(3), 345-361. doi:10.1108/02635570610653498

Chen, W.S. and Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal, 14*(3), 197-235. doi:10.1111/j.1365-2575.2004.00173.x

Chin, W. W. (2010). How to write up and report PLS analyses. In *Handbook of Partial Least Squares,* (pp. 655-690). Berlin, Heidelberg: Springer.

Chun, R. (2005). Ethical character and virtue of organizations: An empirical assessment and strategic implications. *Journal of Business Ethics, (57)*3, 269-284. doi: 10.1007/s10551-004-6591-2

Chun-Chang, L. (2007). Influence of ethics codes on the behavior intention of real estate brokers. *Journal of Human Resource and Adult Learning, 3*(2), 97-106.

Cochran, B. S. G. (1992). Masonry and the Rule of Law Society. *Vox Lucis, 2*(7), 471-477.

Coe, R. (2002). It's the effect size, stupid: What effect size is and why it is important. *Proceedings of the Annual Conference of the British Educational Research Association, Exeter, England,* 1-13.

Coltman, T., Devinney, T. M., Midgley, D. F., & Venaik, S. (2008). Formative versus reflective measurement models: Two applications of formative measurement. *Journal of Business Research, 61*(12), 1250-1262. doi: 10.1016/j.jbusres.2008.01.013

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Information Security Technical Report, 14*(4), 186-196. doi:10.1016/j.istr.2010.04.004

Comrey, A. L., & Lee, H. B. (1992). *A first course in factor analysis*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Creswell, J.W. (2003). *Research design: Qualitative, quantitative, and mixed approaches.* Thousand Oaks, CA: Sage

Crook, R., Ince, D., Lin, L., & Nuseibeh, B. (2002). Security requirements engineering: When anti-requirements hit the fan. *Proceedings of the IEEE Joint International Requirements Engineering Conference (RE'02), Essen, Germany,* 203-205. doi: 10.1109/ICRE.2002.1048527

Cunningham, W. P. (1998). The golden rule as a universal ethical norm. *Journal of Business Ethics, 17*(1), 105-109. doi:10.1023/A:1005752411193

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658. doi:10.1057/ejis.2011.23

D’Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*(1), 59-71. doi: 10.1007/s10551-008-9909-7

D’Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 1-20. doi: 10.1287/isre.1070.0160

Dahlsgaard, K., Peterson, C., Seligman, M. E. P. (2005). Shared virtue: The convergence of valued human strengths across culture and history. *Review of General Psychology, 9*(3), 203-213. doi:10.1037/1089-2680.9.3.203

Dark, M., Harter, N., Morales, L., & Garcia, M. A. (2008). An information security ethics education model. *Journal of Computing Sciences in Colleges, 23*(6), 82-88.

DeCoster, J. (1998). *Overview of factor analysis.* Retrieved from http://www.stat-help.com/factor.pdf

Delaney, J. T., & Sockell, D. (1992). Do company ethics training programs make a difference?: An empirical analysis. *Journal of Business Ethics, 11*(9), 719-727. doi:10.1007/BF01686353

Department of Defense. (2008). *Information Assurance Workforce Improvement Program Manual DoD 8570.01M,* 18-40.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security, 20*(2), 165-172. doi: 10.1016/S0167-4048(01)00209-7

Dhillon, G., & Backhouse, J. (2000). Information system security management in the New Millennium. *Communications of the ACM, 43*(7), 125-128. doi: 10.1145/341852.341877

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153. doi:10.1046/j.1365-2575.2001.00099.x

Dhillon, G., & Silva, L. (2001). Interpreting computer-related crime at the malaria research center. A case study. *Advances in Information and Communication Technology, 72,* 167-182. doi:10.1007/0-306-47007-1_13

Dhillon, G., Tejay, G., & Hong, W. (2007). Identifying governance dimensions to evaluate information systems security in organizations. *Proceedings of the 40th Hawaii International Conference on Systems Sciences (HICSS '07), HI, USA,* 1-9. doi: 10.1109/HICSS.2007.257

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information systems security in organizations. *Information Systems Journal, 16*(3), 293-314. doi: 10.1111/j.1365-2575.2006.00219.x

Diamantopoulos, A. (2011). Incorporating formative measures into covariance-based structural equation models. *MIS Quarterly, 35*(2), 335-358.

Diamantopoulos, A., Riefler, P., & Roth, K. P. (2008). Advancing formative measurement models. *Journal of Business Research, 61*(12), 1203-1218. doi: 10.1016/j.jbusres.2008.01.009

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research, 38*(2), 269-277. doi:10.1509/jmkr.38.2.269.18845

DiStefano, C., & Hess, B. (2005). Using confirmatory factor analysis for construct validation: An empirical review. *Journal of Psychoeducational Assessment, 23*(3), 225-241. doi: 10.1177/073428290502300303

Dodig-Crnkovic, G. & Hofkirchner, W (2011). Floridi's "open problems in philosophy of information". *Information, 2*(2), 327-359. doi:10.3390/info2020327

Donner, M. (2003). The dinosaur and the butterfly: A tale of computer ethics. *IEEE Security & Privacy, 1*(5), 61-63.

Dorantes, C. A., Hewitt, B., & Goles, T. (2006). Ethical decision-making in an IT context: The roles of personal moral philosophies and moral intensity. *Proceedings of the 39th Hawaii International Conference on Systems Sciences (HICSS '06), HI, USA,* 1-10. doi:10.1109/HICSS.2006.161

Dow, K. E., Wong, J., Jackson, C., & Leitch, R. A. (2008). A comparison of structural equation modeling approaches: The case of user acceptance of information systems. *Journal of Computer Information Systems, 48*(4), 106-114.

Drover, W., Franczak, J., & Beltramini, R. F. (2012). A 30-Year historical examination of ethical concerns regarding business ethics: Who's concerned? *Journal of Business Ethics, 111*(4), 431-438. doi:10.1007/s10551-012-1214-9

Duarte, F. (2008). "What we learn today is how we behave tomorrow": A study on students' perceptions of ethics in management education. *Social Responsibility Journal, 4*(1/2), 120-128. doi:10.1108/17471110810856884

Dunkerley, K. D., & Tejay, G. (2011). A confirmatory analysis of information systems security success factors. *Proceedings of the 44th Hawaii International Conference on Systems Sciences (HICSS '11), HI, USA,* 1-10. doi:10.1109/HICSS.2011.5

Dyck, B., & Kleysen, R. (2001). Aristotle's virtues and management thought: An empirical exploration of an integrative pedagogy. *Business Ethics Quarterly, 11*(4), 561-574. doi:10.2307/3857761

Dyck, B., & Wong, K. (2010). Corporate spiritual disciplines and the quest for organizational virtue. *Journal of Management, Spirituality & Religion, 7*(1), 7-29. doi:10.1080/14766080903497565

Edwards, J. R. (2001). Multidimensional constructs in organizational behavior research: An integrative analytical framework. *Organizational Research Methods, 4*(2), 144-192. doi: 10.1177/109442810142004

Ekelhart, A., Fenz, S., & Neubauer, T. (2009). AURUM: A framework for information security risk management. *Proceedings of the 42nd Hawaii International Conference on Systems Sciences (HICSS '09), HI, USA,* 1-10.

Ellis, P. D. (2010). *The essential guide to effect sizes: Statistical power, meta-analysis, and the interpretation of research results.* Cambridge, NY: Cambridge University Press.

Eloff, J., & Eloff, M. (2003). Information security management – A new paradigm. *Proceedings of the South African Institute of Computer Scientists and Information Technologists (SAICSIT 2003), Wilderness, South Africa,* 130-136.

Ess, C. (2008). Luciano Floridi's philosophy of information and information ethics: Critical reflections and the state of the art. *Ethics and Information Technology,10*(2-3), 89-96. doi:10.1007/s10676-008-9172-8

Evans, S., Heinbuch, D., Kyle, E., Piorkowski, J., & Wallener, J. (2004). Risk-based System security engineering: Stopping attacks with intention. *IEEE Security & Privacy,* 2(6), 59–62. doi:10.1109/MSP.2004.109

Falkenberg, L., & Herremans, I. (1995). Ethical behaviours in organizations: Directed by the formal or informal systems? *Journal of Business Ethics*, *14*(2), 133-143. doi: 10.1007/BF00872018

Ferguson, C. W. (1979). *Fifty million brothers: A panorama of American lodges and clubs*. Westport, CT: Greenwood Press.

Finstad, K. (2010). Response interpolation and scale sensitivity: Evidence against 5-point scales. *Journal of Usability Studies, 5*(3), 104-110.

Floridi. L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology, 1*(1), 37–56. doi: 10.1023/A:1010018611096

Floridi, L. (2006). Information ethics, its nature and scope. *Computers and Society, 36*(3), 21-36. doi:10.1145/1195716.1195719

Floridi, L. (2010). Ethics after the information revolution. In L. Floridi (Ed.), *The Cambridge Handbook of Information and Computer Ethics*, (pp. 3-19). Cambridge, NY: Cambridge University Press.

Floridi, L., & Sanders, J. W. (2002). Mapping the foundationalist debate in computer ethics. *Ethics and Information Technology, 4*(1), 1-9. doi: 10.1023/A:1015209807065

Floridi, L., & Sanders, J. W. (2005). Internet ethics: The constructionist values of Homo Poieticus. In Cavalier, R. (Ed) *The impact of the internet on our moral lives,* 195-214. New York: SUNY Press.

Fornell, C. & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Fowler, F. J. (2014). Survey research methods. Los Angles: Sage Publications, Inc.

Freeze, R. D., & Rasche, R. L. (2007). *An assessment of formative and reflective constructs in IS research.* Unpublished paper. W. P. Carey School of business. Arizona State University.

Freeze, R. D., & Rasche, R. L. (2011). Construct transportability: A choice that matters. *Proceedings of the 44th Hawaii International Conference on Systems Sciences (HICSS ’11), HI, USA,* 1-10.

Gagne, P., & Hancock, G. R. (2006). Measurement model quality, sample size, and solution propriety in confirmatory factor models. *Multivariate Behavioral Research, 41*(1), 65-83. doi:10.1207/s15327906mbr4101_5

Gefen, D. & Straub, D., (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*(1), 91-109.

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*(1), 16-30. doi:10.1016/j.cose.2004.11.002

Gerber, M., & von Solms, R. (2008). Information security requirements – interpreting the legal aspects. *Computers & Security, 27*(5-6), 124-135. doi: 10.1016/j.cose.2008.07.009

Goodman, C. M. (1987). The Delphi technique: A critique. *Journal of Advanced Nursing, 12*(6), 729-734. doi:10.1111/j.1365-2648.1987.tb01376.x

Gray, J. M. (2013). *Development of virtue ethics based information system security formative constructs for information systems trusted workers.* Unpublished manuscript, Graduate School of Computer and Information Sciences, Nova Southeastern University, Fort Lauderdale, FL, USA.

Gray, J. M., & Tejay. G. (2014). Development of virtue ethics based security constructs for information systems trusted workers. *Proceedings of the 9th International Conference on Cyber Warfare and Security (ICCWS-2014), West Lafayette, IN, USA*, 256-264. doi:10.13140/2.1.1946.4328

Gray, J. M., & Tejay, G. (2015). *Introducing virtue ethics concepts into the decision making processes of information system security trusted workers: A Delphi study.* Manuscript submitted for publication.

Greenberg, J. (2002). Who stole the money? Individual and situational determinants of employee theft. *Organizational Behavior and Human Decision Processes, 89*, 985–1003. doi:10.1016/S0749-5978(02)00039-0

Greenemeier, L., & Gaudin, S. (2007). The threat from within – Insiders represent one of the biggest security risks because of their knowledge and access. To head them off, consider the psychology and technology behind the attacks. *Insurance & Technology*, *32*(2), 38-41.

Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider attacks. *Journal of Strategic Security, 4* (2), 25-48. doi:10.5038/1944-0472.4.2.2

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *Security & Privacy, 6*(1), 61-64. doi:10.1109/MSP.2008.8

Grodzinsky, F. S. (2001). The practitioner from within: revisiting the virtues. In R. A. Spinello, & H. T. Tavani (Eds.), *Readings in Cyberethics* (pp. 580-592). Sudbury, MA: Jones and Bartlett.

Hall, R. J., Snell, A. F., & Foust, M. S. (1999). Item parceling strategies in SEM: Investigating the subtle effects of unmodeled secondary constructs. *Organizational Research Methods, 2*(3), 233-256. doi: 10.1177/109442819923002

Haines, R., & Leonard, L. N. (2007). Situational influences on ethical decision-making in an IT context. *Information & Management, 44*(3), 313-320. doi: 10.1016/j.im.2007.02.002

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2009). *Multivariate data analysis*. Upper Saddle River, NJ: Prentice Hall.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139-152. doi: 10.2753/MTP1069-6679190202

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, *40*(3), 414-433. doi: 10.1007/s11747-011-0261-6

Harrington, S. J. (1991). What corporate America is teaching about ethics. *Academy of Management Executive, 5*(1), 21-30. doi:10.5465/AME.1991.4274711

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278. doi:10.2307/249656

Harris, C. E. (2008). The good engineer: Giving virtue its due in engineering ethics. *Science and Engineering Ethics, 14*(2), 153-164. doi:10.1007/s11948-008-9068-3

Hart, D. K. (2001). Administration and the ethics of virtue: In all things, choose first for good character and then for technical expertise. In T. L. Cooper (Ed.), *Handbook of Administrative Ethics,* (pp. 131 – 150). New York: Marcel Dekker, Inc.

Hayduk, L., Cummings, G., Boadu, K., Pazderka-Robinson, H., & Boulianne, S. (2007). Testing! Testing! One, two, three–testing the theory in structural equation models! *Personality and Individual Differences, 42*(5), 841-850. doi:10.1016/j.paid.2006.10.001

Henson, R. K., & Roberts, J. K. (2006). Use of exploratory factor analysis in published research common errors and some comment on improved practice. *Educational and Psychological measurement*, *66*(3), 393-416. doi: 10.1177/0013164405282485

Herath, T., Herath, H., & Bremser, W. G. (2010). Balanced scorecard implementation of security strategies: a framework for IT security performance management. *Information Systems Management, 27*(1), 72-81. doi: 10.1080/10580530903455247

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. doi:10.1016/j.dss.2009.02.005

Hilton, T. (2000). Information systems ethics: A practitioner survey. *Journal of Business Ethics, 28*(4), 279-284. doi:10.1023/A:1006274825363

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of Management, 21*(5), 967-988. doi:10.1016/0149-2063(95)90050-0

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational research methods, 1*(1), 104-121. doi: 10.1177/109442819800100106

Hollinger, R. C., & Clark, J. P. (1982). Formal and informal social controls of employee deviance. *The Sociological Quarterly*, *23*(3), 333-343. doi:10.1111/j.1533-8525.1982.tb01016.x

Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural equation modelling: Guidelines for determining model fit. *Electronic Journal of Business Research Methods, 6*(1), 53-60.

Howe, E. (1990). Normative ethics in planning. *Journal of Planning Literature, 5*(2), 123-150. doi:10.1177/088541229000500201

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security – A neo-institutional perspective. *Journal of Strategic Information Systems, 16(*2), 153-172. doi:10.1016/j.jsis.2007.05.004

Huff, C., & Frey W. (2005). Moral pedagogy and practical ethics. *Science and Engineering Ethics, 11*(3), 389-408. doi:10.1007/s11948-005-0008-1

Huff, C., Barnard, L., & Frey, W. (2008a). Good computing: A pedagogically focused model of virtue in the practice of computing (part 1). *Journal of Information, Communication and Ethics in Society*, *6*(3), 246-278. doi: 10.1108/14779960810916246

Huff, C., Barnard, L., & Frey, W. (2008b). Good computing: a pedagogically focused model of virtue in the practice of computing (part 2). *Journal of Information, Communication and Ethics in Society*, *6*(4), 284-316. doi: 10.1108/14779960810921114

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats, an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2*(1), 4-27.

Hyrkäs, K., Appelqvist-Schmidlechner, K., & Oksa, L. (2003). Validating an instrument for clinical supervision using an expert panel. *International Journal of Nursing Studies, 40*(6), 619-625. doi:10.1016/S0020-7489(03)00036-1

Iivari, J. (1991). A paradigmatic analysis of contemporary schools of IS development. *European Journal of Information Systems, 1*(4), 249-272. doi: 10.1057/ejis.1991.47

Iivari, J. (2007). A paradigmatic analysis of information systems as a design science. *Scandinavian Journal of Information Systems, 19*(2), 39.

Jabbour, G., & Menascé, D. (2009). The insider threat security architecture: A framework for an integrated, inseparable, and uninterrupted self-protection mechanism. *Proceedings of the 12th IEEE International Conference on Computational Science and Engineering (CSE'09). Vancouver,Canada, 3*, 244-251. doi: 10.1109/CSE.2009.278

Jackson, T. (2000). Management ethics and corporate policy: A cross-cultural comparison. *Journal of Management Studies, 37*(3), 349-369. doi:10.1111/1467-6486.00184

Jackson, D. L., Gillaspy Jr, J. A., & Purc-Stephenson, R. (2009). Reporting practices in confirmatory factor analysis: an overview and some recommendations. *Psychological Methods, 14*(1), 6-23. doi: 0.1037/a0014694

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199-218. doi:10.1086/376806

Jones, A. (2007). A framework for the management of information security risks. *BT Technology Journal, 25*(1), 30-36. doi:10.1007/s10550-007-0005-9

Jones, T. M. (1991). Ethical decision making by individuals in organizations: An issue-contingent model. *Academy of Management Review, 16*(2), 366-395. doi: 10.2307/258867

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154. doi:10.1016/S0268-4012(02)00105-6

Kane, J., & Patapan, H. (2006). In search of prudence: The hidden problem of managerial reform. *Public Administration Review, 66*(5), 711-724. doi:10.1111/j.1540-6210.2006.00636.x

Kaptein, M. (1998). *Ethics management: Auditing and developing the ethical content of organizations.* Dordrecht, Netherlands: Kluwer Academic Publishers. doi: 10.1007/978-94-011-4978-5

Kaptein, M. (2008). Developing a measure of unethical behavior in the workplace: A stakeholder perspective. *Journal of Management, 34*(5), 978-1008. doi: 10.1177/0149206308318614

Kaptein, M., & Schwartz, M. S. (2008). The effectiveness of business codes: A critical examination of existing studies and the development of an integrated research model. *Journal of Business Ethics, 77*(2), 111-127. doi:10.1007/s10551-006-9305-0

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security, 24*(3), 246-260. doi: 10.1016/j.cose.2004.08.011

Keller, A. C., Smith, K. T., & Smith, L. M. (2007). Do gender, education level, religiosity, and work experience affect the ethical decision-making of U. S. accountants? *Critical Perspectives on Accounting, 18*(3), 299-314. doi: 10.1016/j.cpa.2006.01.006

Ketel, M. (2008). IT security risk management. *Proceedings of the 46th Annual Southeast Regional Conference (ACMSE 46), Auburn, AL, USA,* 373-376. doi: 10.1145/1593105.1593203

Kim, H. Y. (2013). Statistical notes for clinical researchers: assessing normal distribution (2) using skewness and kurtosis. Restorative dentistry & endodontics, 38(1), 52-54. doi: 10.5395/rde.2013.38.1.52

King, W. R., & He, J. (2005). External validity in IS survey research. *Communications of the Association for Information Systems*, *16,* 880-894.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67-94. doi:10.2307/249410

Kline, R. B. (1998). *Principles and practice of structural equation modeling.* NY, NY: Guilford Press.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*(7), 509-520. doi:10.1016/j.cose.2009.04.006

Kutner, M. H., Nachtsheim, C. J., Neter, J., & Li, W. (2005). *Applied linear statistical models*. New York: McGraw-Hill Education

Lancaster, G. A., Dodd, S., & Williamson, P. R. (2004). Design and analysis of pilot studies: recommendations for good practice. *Journal of Evaluation in Clinical Practice, 10(*2), 307-312. doi: 10.1111/j..2002.384.doc.x

Landau, S. (2013) Making Sense from Snowden*. Security & Privacy, IEEE, 11*(4), 66-75. doi:10.1109/MSP.2013.90

Lange, M., Mendling, J., & Recker, J. (2012). Realizing benefits from enterprise architecture: a measurement model. *Proceedings of the 20th European Conference on Information Systems (ECIS 12),Barcelona, Spain,* 1-12.

Leach, J. (2003). Improving user security behavior. *Computers & Security, 22*(8), 685-692. doi:10.1016/S0167-4048(03)00007-5

Lease, D. R. (2006). *From great to ghastly: How toxic organizational cultures poison companies – The rise and fall of Enron, WorldCom, HealthSouth, and Tyco International.* Unpublished paper, Academy of Business, Norwich University.

LeBreton, J. M., & Sentor, J. L. (2008). Answers to 20 questions about interrater reliability and interrater agreement. Organizational Research Methods, 11(4), 815-852. doi:10.1177/1094428106296642

Leedy, P. D., & Ormrod, J. E. (2005). *Practical research. Planning and design.* Upper Saddle River, NJ: Pearson Merrill Prentice Hall.

Lee, A. S., & Hubona, G. S. (2009). A scientific basis for rigor in information systems research. *MIS Quarterly, 33*(2), 237-262.

Lenth, R. V. (2001). Some practical guidelines for effective sample size determination. *The American Statistician, 55*(3), 187-193. doi:10.1198/000313001317098149

Leonard, L. N., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management*, *42*(1), 143-158. doi: 10.1016/j.im.2003.12.008

Lewis, B. R., Templeton, G. F., & Byrd, T. A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems, 14*(4), 388-400. doi:10.1057/palgrave.ejis.3000552

Liebenau, J., & Backhouse, J. (1990). *Understanding information: an introduction.* London: Palgrave Macmillan.

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. *Proceedings of the 7th Australian Information Security Management Conference, Perth, Australia*, 88-97.

Lind, D. A., Marchal, W. G., & Wathen, S. A. (2008). *Statistical techniques in business & economics.* New York: McGraw-Hill Irwin.

Loch, K. D., & Conger, S. (1996). Evaluating ethical decision making and computer use. *Communications of the AC*M, *39*(7), 74-83. doi:10.1145/233977.233999

Lummus, R. R., Vokurka, R. J., & Duclos, L. K. (2005). Delphi study on supply chain flexibility. *International Journal of Production Research, 43*(13), 2687-2708. doi:10.1080/00207540500056102

Lynn, M. R. (1986). Determination and quantification of content validity. *Nursing Research, 35*(6), 382-386. doi:10.1097/00006199-198611000-00017

Ma, Q., & Pearson, J. M. (2005). ISO 17799: “Best practices” in information security management? *Communications of the Association for Information Systems, 15*(1), 576-591.

MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. *Psychological Methods, 4*(1), 84-99. doi:10.1037//1082-989X.4.1.84

MacIntyre, A. (1984). *After virtue: A study in moral theory* (2nd Ed.). Notre Dame, IN: University of Notre Dame Press.

MacKenzie, S. B., Podsakoff, P. M., & Jarvis, C. B. (2005). The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. *Journal of Applied Psychology, 90*(4), 710-730. doi: 10.1037/0021-9010.90.4.710

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*(2), 293-334.

Magklaras, G. B., Furnell, S. M., & Brooke, P. J. (2006). Towards an insider threat prediction specification language. *Information Management & Computer Security,14*(4), 361-381. doi:10.1108/09685220610690826

Magnan, S. W. (2000). Safeguarding information operations. *Studies in Intelligence, Summer 2000*(9). Retrieved from https://www.cia.gov

Marino, K. (2008). Former systems administrator gets 30 months in prison for planting "Logic Bomb" in company computers. *United States Department of Justice News Release lin1208.rel.* Retrieved from http://www.usdoj.gov/usao/nj/press/index. html

Mathieson, K. (2008). Making ethics easier. *Computer, 41*(7), 91-93. doi: 10.1109/MC.2008.230

Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T. & Longstaff, T. (2005). Analysis and detection of malicious insiders. *International Conference on Intelligence Analysis, McLean, VA, USA*, 1-8.

McDevitt, R., Giapponi, C., & Tromley, C. (2007). A model of ethical decision making: The integration of process and content. *Journal of Business Ethics, 73*(2), 219-229. doi:10.1007/s10551-006-9202-6

McDonald, R. P., & Ho, M. H. R. (2002). Principles and practice in reporting structural equation analyses. *Psychological methods, 7*(1), 64-82.

Mehigan, T., & De Burgh, H. (2008). 'Aufklarung', freemasonry, the public sphere and the question of Enlightenment. *Journal of European Studies, 38*(1), 5-25. doi: 10.1177/0047244107086798

Moor, J. H. (1985). What is computer ethics? *Metaphilosophy, 16*(4), 266-275. doi: 10.1111/j.1467-9973.1985.tb00173.x

Moor, J. H. (1998a). Reason, relativity, and responsibility in computer ethics. *Computers and Society, 28*(1), 14-21. doi:10.1145/277351.277355

Moor, J. H. (1998b). If Aristotle were a computer professional. *Computers and Society, 28*(3), 13-16. doi:10.1145/298972.298977

Moore, G. (2005a). Humanizing business: A modern virtue ethics approach. *Business Ethics Quarterly, 15*(2), 237-255. doi:10.5840/beq200515212

Moore, G. (2005b). Corporate character: Modern virtue ethics and the virtuous corporation. *Business Ethics Quarterly, 15*(4), 659-685. doi: 10.5840/beq200515446

Munshi, J. (2014). A method for constructing Likert scales. Retrieved from http://ssrn.com/abstract=2419366. doi: 10.2139/ssrn.2419366

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18*(2), 126-139. doi: 10.1057/ejis.2009.10

Nash, L. (1990). *Good intentions aside: A manager's guide to resolving ethical problems.* Cambridge, MA: Harvard Business School Press.

National Institute of Standards and Technology. (2006). *Guide for developing security plans for federal Information Systems* (Special Publication 800-18).

Newstrom, J. W., & Ruch, W. A. (1975). The ethics of management and the management of ethics. *MSU Business Topics*, *23*(1), 29-37.

Nunnally, J.C., & Bernstein, I.H. (1994). *Psychometric theory*. New York: McGraw-Hill.

Oderberg, D. S. (1999). On the cardinality of the cardinal virtues. *International Journal of Philosophical Studies*, *7*(3), 305-322. doi:10.1080/096725599341785

Okolica, J. S., Peterson, G. L., & Mills, R. F. (2008). Using PLSI-U to detect insider threats by datamining e-mail. *International Journal of Security and Networks, 3*(2), 114-121. doi:10.1504/IJSN.2008.017224

Pahnila, S., & Siponen, M., & Mahmood, A. (2007). Employee's behavior towards IS security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS '07), HI, USA*, 1-10. doi: 10.1109/HICSS.2007.206

Parboteeah, K. P., Hoegl, M., & Cullen, J. B. (2008). Ethics and religion: An empirical test of a multidimensional model. *Journal of Business Ethics*, *80*(2), 387-398. doi:10.1007/s10551-007-9439-8

Peter, J. P. (1981). *Construct validity: A review of basic issues and marketing practices. Journal of Marketing Research,18*(2), 133-145.

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly, 31*(4), 623-656.

Pieper, J. (1966). *The four cardinal virtues.* Notre Dame, IN: University of Notre Dame Press.

Pinsonneault, A., & Kraemer, K. L. (1993). Survey research methodology in management information systems: An assessment. *Journal of Management Information Systems, 10*(2), 75-105.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of applied psychology, 88*(5), 879. doi: 10.1037/0021-9010.88.5.879

Pollack, T. A., & Hartzel, K. A. (2006). Ethical and legal issues for the information systems professional. *Proceedings of the 2006 ASCUE Conference, Myrtle Beach, SC, USA*, 172-179.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector.* Technical Report CMU/SEI-2004-TR-021, Carnegie Mellon University, Software Engineering Institute.

Rea, L. M., & Parker, R. A. (2005). *Designing and conducting survey research: A comprehensive guide.* San Francisco: John Wiley & Sons.

Reitz, J. M. (2004) *Dictionary for Library and Information Science.* Westport, CT: Libraries Unlimited.

Riggio, R. E., Zhu, W., Reina, C. & Maroosis, J. A. (2010). Virtue-based measurement of ethical leadership: the leadership virtues questionnaire. *Consulting Psychology Journal: Practice and Research, 62*(4), 235-50. doi:10.1037/a0022286

Roberts, E. S. (1999). In defence of the survey method: An illustration from a study of user information satisfaction. *Accounting & Finance, 39*(1), 53-77. doi: 10.1111/1467-629X.00017

Robertson, C., & Fadil, P. A. (1999). Ethical decision making in multinational organizations: A culture-based model. *Journal of Business Ethics, 19*(4), 385-392. doi:10.1023/A:1005742016867

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.

Salkind, N. J. (2009). *Exploring Research.* Upper Saddle River, NJ: Prentice Hall.

Sauro, J. (2014). Should you use 5 or 7 point scales? Retrieved from http://www.measuringusability.com/blog/scale-points.php

Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online*, *8*(2), 23-74.

Schervish, M. J. (1996). P values: what they are and what they are not. *The American Statistician, 50*(3), 203-206.

Schminke, M., Ambrose, M. L., & Neubaum, D. O. (2005). The effect of leader moral development on ethical climate and employee attitudes. *Organizational Behavior and Human Decision Processes*, *97*(2), 135-151. doi: 10.1016/j.obhdp.2005.03.006

Schmitt, N., & Stults, D. M. (1985). Factors defined by negatively keyed items: The result of careless respondents? *Applied Psychological Measurement*, *9*(4), 367-373. doi:10.1177/014662168500900405

Schneider, B., & Reichers, A. E. (1983). On the etiology of climates. *Personnel Psychology, 36*(1), 19-39. doi:10.1111/j.1744-6570.1983.tb00500.x

Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting structural equation modeling and confirmatory factor analysis results: A review. *The Journal of Educational Research, 99*(6), 323-338. doi: 10.3200/JOER.99.6.323-338

Schumacker, R. E., & Lomax, R. G. (1996). *A beginner's guide to structural equation modeling.* Mahwah, NJ: Lawrence Erlbaum Associates.

Schweitzer, M. E., Ordóñez, L., & Douma, B. (2004). Goal setting as a motivator of unethical behavior. *Academy of Management Journal*, *47*(3), 422-432. doi: 10.2307/20159591

Sekaran, U., & Bougie, R. (2010). *Research methods for business: A skill building approach.* West Sussex, United Kingdom: John Wiley & Sons, Ltd.

Shanahan, K. J., & Hyman, M. R. (2003). The development of a virtue ethics scale. *Journal of Business Ethics, 42*(2), 197-208. doi:10.1023/A:1021914218659

Sharma, S., Mukherjee, S., Kumar, A., & Dillon, W. R. (2005). A simulation study to investigate the use of cutoff values for assessing model fit in covariance structure models. *Journal of Business Research, 58*(7), 935-943.

Simga-Mugan, C., Daly, B. A., Onkal, D., & Kavut, L. (2005). The influence of nationality and gender on ethical sensitivity: An application of the issue-contingent model. *Journal of Business Ethics, 57*(2), 139-159.

Singh, J. B. (2011). Determinants of the effectiveness of corporate codes of ethics: An empirical study. *Journal of Business Ethics, 101*(3), 385-395. doi: 10.1007/s10551-010-0727-3

Singhapakdi, A., Vitell, S. J., Rallapalli, K. C., & Kraft, K. L. (1996). The perceived role of ethics and social responsibility: A scale development. *Journal of Business Ethics, 15*(11),1131-1140. doi:10.1007/BF00412812

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41. doi: 10.1108/09685220010371394

Siponen, M. (2004). A pragmatic evaluation of the theory of information ethics. *Ethics and Information Technology, 6*(4), 279-290. doi:10.1007/s10676-005-6710-5

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM, 49*(8), 97-100. doi: 10.1145/1145287.1145316

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(7), 445-472.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71. doi: 10.1109/MC.2010.35

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502.

Sison, A. J. G., Hartman, E. M., & Fontrodona, J. (2012). Reviving tradition: Virtue and the common good in business and management. *Business Ethics Quarterly, 22*(2), 207-210. doi:10.5840/beq201222217

Skarlicki, D. P., Folger, R., & Tesluk, P. (1999). Personality as a moderator in the relationship between fairness and retaliation. *Academy of Management Journal, 42*(1), 100-108. doi:10.2307/256877

Sogbesan, A., Ibidapo, A., Zavarsky, P., Ruhl, R., & Lindskog, D. (2012). Collusion threat profile analysis: Review and analysis of MERIT model. *Proceedings of the World Congress on Internet Security (WorldCIS-2012), Ontario, Canada*, 212-217.

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education, 6*, 1-21.

Spelman, H. J. (1996). Dissertations at the grandmaster's festival. *Transactions of the Illinois Lodge of Research, 8*(1), 22-25.

Stage, F. K., Carter, H. C., & Nora, A. (2004). Path analysis: An introduction and analysis of a decade of research. *Journal of Educational Research,* 98(1), 5-13. doi:10.3200/JOER.98.1.5-13

Stamatellos, G. (2011a). Computer ethics and Neoplatonic virtue: A reconsideration of cyberethics in the light of Plotinus' ethical theory. *International Journal of Cyber Ethics in Education, 1*(1), 1-11. doi:10.4018/ijcee.2011010101

Stamatellos, G. (2011b). Virtue, privacy and self-determination: A Plotinian approach to the problem of information privacy. *International Journal of Cyber Ethics in Education, 1*(4), 35-41. doi:10.4018/ijcee.2011100104

Steinmetz, G. H. (1976). *Freemasonry, its hidden meaning.* Richmond, VA: Macoy Publishing and Masonic Supply Company.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169. doi:10.2307/248922

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276. doi:10.1287/isre.1.3.255

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems, 13*(1), 380-427.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469. doi: 10.2307/249551

Streiner, D. L. (2005). Finding our way: An introduction to path analysis. *The Canadian Journal of Psychiatry, 50*(2), 115-122.

Stritzke, W. G., Nguyen, A., & Durkin, K. (2004). Shyness and computer-mediated communication: A self-presentational theory perspective. *Media Psychology, 6*(1), 1-22. doi: 10.1207/s1532785xmep0601_1

Sun, J. (2005). Assessing goodness of fit in confirmatory factor analysis. *Measurement and Evaluation in Counseling and Development, 37*(4), 240-256.

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems, 22*(4), 109-142. doi: 10.2753/MIS0742-1222220405

Swain, S. D., Weathers, D., & Niedrich, R. W. (2008). Assessing three sources of misresponse to reversed Likert items. *Journal of Marketing Research, 45*(1), 116-131. doi:10.1509/jmkr.45.1.116

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2,* 53-55. doi:10.5116/ijme.4dfb.8dfd

Taylor, P. (2008). Insider threat-The fraud that puts companies at risk. *Information Systems Control Journal, 1,* 46-47.

Tenenhaus, M. (2008). Component-based structural equation modelling. *Total Quality Management*, *19*(7-8), 871-886. doi: 10.1080/14783360802159543

Terrell, S. R. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data.* New York: The Guilford Press.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24*(6), 472-484. doi:10.1016/j.cose.2005.05.002

Thong, J. Y. L., Yap, C. S., & Raman, K. S. (1996). Top management support, external expertise and information systems implementation in small businesses. *Information Systems Research, 7*(2), 248-267. doi:10.1287/isre.7.2.248

Treiblmaier, H., Bentler, P. M., & Mair, P. (2011). Formative constructs implemented via common factors. *Structural Equation Modeling, 18*(1), 1-17. doi: 10.1080/10705511.2011.532693

Trevino, L. K. (1986). Ethical decision making in organizations: A person-situation interactionist model. *Academy of management Review*, *11*(3), 601-617. doi: 10.2307/258313

Trevino, L. K. (1990). A cultural perspective on changing and developing organizational ethics. *Research in organizational change and development, 4,* 195-230.

Trevino, L. K., Hartman, L. P., & Brown, M. (2000). Moral person and moral manager: How executives develop a reputation for ethical leadership. *California Management Review, 42*(4), 128-142. doi:10.2307/41166057

Trevino, L. K., & Weaver, G. R. (1994). Business ETHICS/BUSINESS ethics: One field or two? *Business Ethics Quarterly, 4*(2), 113-128. doi:10.2307/3857484

Trevino, L. K., Weaver, G. R., Gibson, D. G., & Toffler, B. L. (1999). Managing ethics and legal compliance: What works and what hurts. *California Management Review, 41*(2). doi:10.2307/41165990

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*, *48*(6), 1143-1158. doi: 10.5465/AMJ.2005.19573114

Van Niekerk, J. F., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486. doi: 10.1016/j.cose.2009.10.005

van Teijlingen, E., & Hundley, V. (2002). The importance of pilot studies. *Nursing Standard*, *16*(40), 33-36. doi:10.7748/ns2002.06.16.40.33.c3214

von Solms, B. (2000). Information security – the third wave? *Computers & Security, 19*(7), 615-620. doi:10.1016/S0167-4048(00)07021-8

von Solms, B. (2006). Information security–the fourth wave. *Computers & security, 25*(3), 165-168. doi:10.1016/j.cose.2006.03.004

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376. doi: 10.1016/j.cose.2004.05.002

von Solms, S. H. (2005). Information security governance – compliance management vs operational management. *Computers & Security, 24*(6), 443-447. doi: 10.1016/j.cose.2005.07.003

Vroom, C., & von Solms, R. (2004). Towards informational security behavioral compliance. *Computers & Security, 23*(3), 191-198. doi: 10.1016/j.cose.2004.01.012

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267-284. doi: 10.1057/ejis.2010.72

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101-105. doi:10.1057/ejis.2009.12

Webley, S., & Werner, A. (2008). Corporate codes of ethics: Necessary but not sufficient. *Business Ethics: A European Review, 17*(4), 405-415. doi: 10.1111/j.1467-8608.2008.00543.x

Weber, J. (1981). Institutionalizing ethics into the corporation. *MSU Business Topics, 29*(2), 47-52.

Weber, J. (1993). Institutionalizing ethics into business organizations: a model and research agenda. *Business Ethics Quarterly, 3*(4), 419-436. doi:10.2307/3857287

Weber, J. (2010). Moral reasoning in the business context: A view from my rocking chair. *Journal of Organizational Moral Psychology, 1*(2), 55-76.

Weber, J., & Gillespie, J. (1998). Differences in ethical beliefs, intentions, and behaviors: The role of beliefs and intentions in ethics research revisited. *Business & Society, 37*(4), 447-467. doi:10.1177/000765039803700406

Weijters, B., Cabooter, E., & Schillewaert, N. (2010). The effect of rating scale format on response styles: The number of response categories and response category labels. *International Journal of Research in Marketing, 27*(3), 236-247. doi: 10.1016/j.ijresmar.2010.02.004

Whetstone, J. T. (2001). How virtue fits within business ethics. *Journal of Business Ethics, 33*(2), 101-114. doi:10.1023/A:1017554318867

Whetstone, J. T. (2003). The language of managerial excellence: Virtues as understood and applied. *Journal of Business Ethics, 44*(4), 343-357. doi: 10.1023/A:1023640401539

Whetstone, J. T. (2005). A framework for organizational virtue: The interrelationship of mission, culture, and leadership. *Business Ethics: A European Review, 14*(4), 367-378. doi:10.1111/j.1467-8608.2005.00418.x

Wiant, T. L. (2005). Information security policy's impact on reporting security incidents. *Computers & Security, 24*(6), 448-459. doi:10.1016/j.cose.2005.03.008

Williams, L. J., Edwards, J. R., & Vandenberg, R. J. (2003). Recent advances in causal modeling methods for organizational and management research. *Journal of Management, 29*(6), 903-936. doi: 10.1016/S0149-2063_03_00084-9

Wood-Harper, A. T., Corder, S., Wood, J. R. G., & Watson, H. (1996). How we profess: The ethical systems analyst. *Communications of the ACM, 39*(3), 69-77. doi: 10.1145/227234.227244

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology, 58*(2), 212-222. doi:10.1002/asi.20474

Wu, X., Rogerson, S., & Fairweather, N. (2001). Being ethical in developing information systems: An issue of methodology or maturity in judgment? *Proceedings of the 34th Annual Hawaii International Conference on System Sciences (HICSS-34), HI, USA*, 8037-8045.

Yusof, Z. M., Basri, M., & Zin, N. A. M. (2010). Classification of issues underlying the development of information policy. *Information Development, 26*(3), 204-213. doi:10.1177/0266666910368218

Zeadally, S., Yu, B., Jeong, D. H., & Liang, L. (2012). Detecting insider threats: Solutions and trends. *Information Security Journal: A Global Perspective, 21*(4), 183-192. doi: 10.1080/19393555.2011.654318